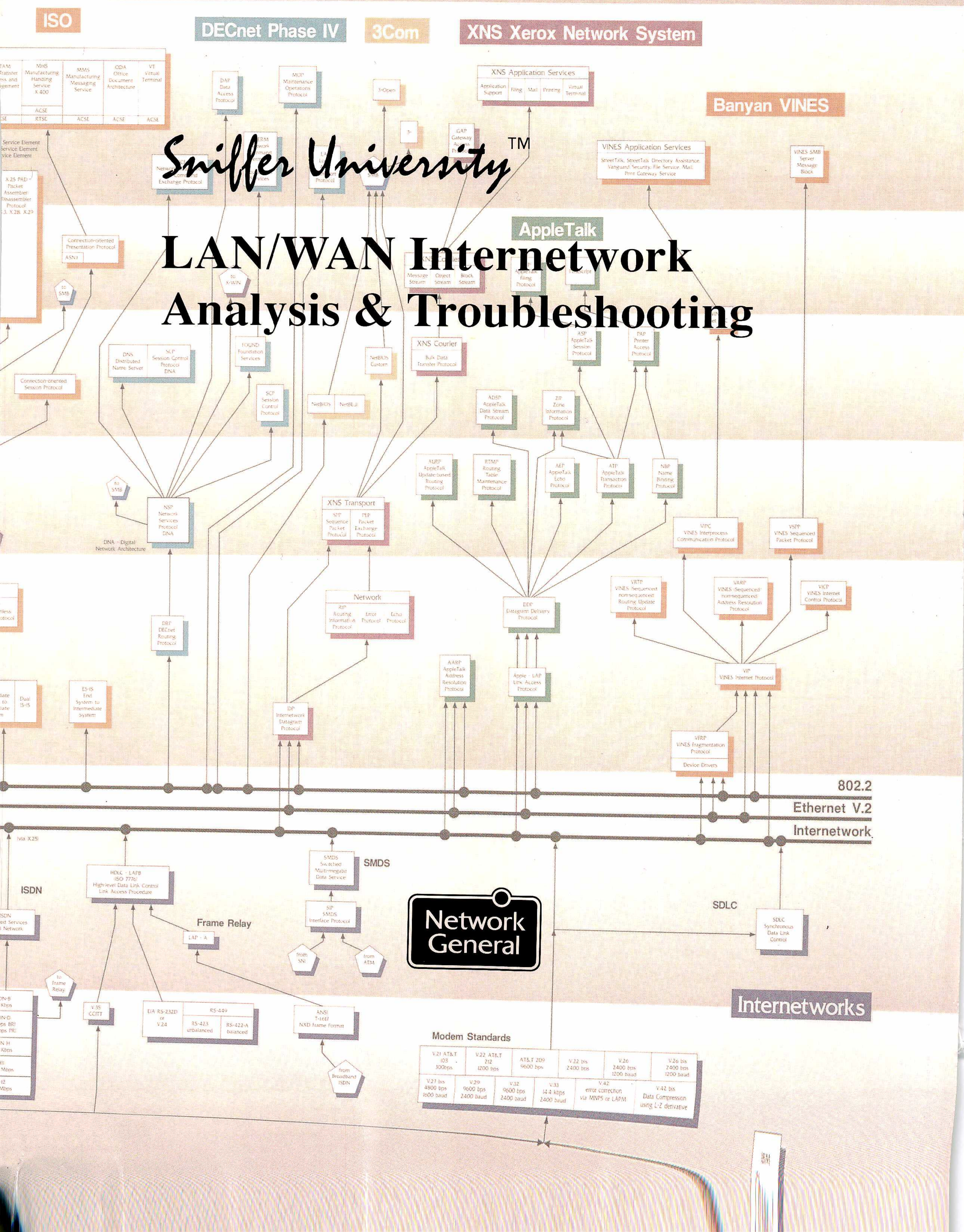
Sniffer University™

LAN/WAN Internetwork Analysis & Troubleshooting



Network General

Internetwork Analysis and Troubleshooting

SNIFFER® UNIVERSITY

Overview 1 - 1

Internetwork Analysis and Troubleshooting, 10/96 Rev 5.0

Network General

Network General

Sniffer University

Housekeeping

BREAKS

LUNCH

TELEPHONES

REST ROOMS

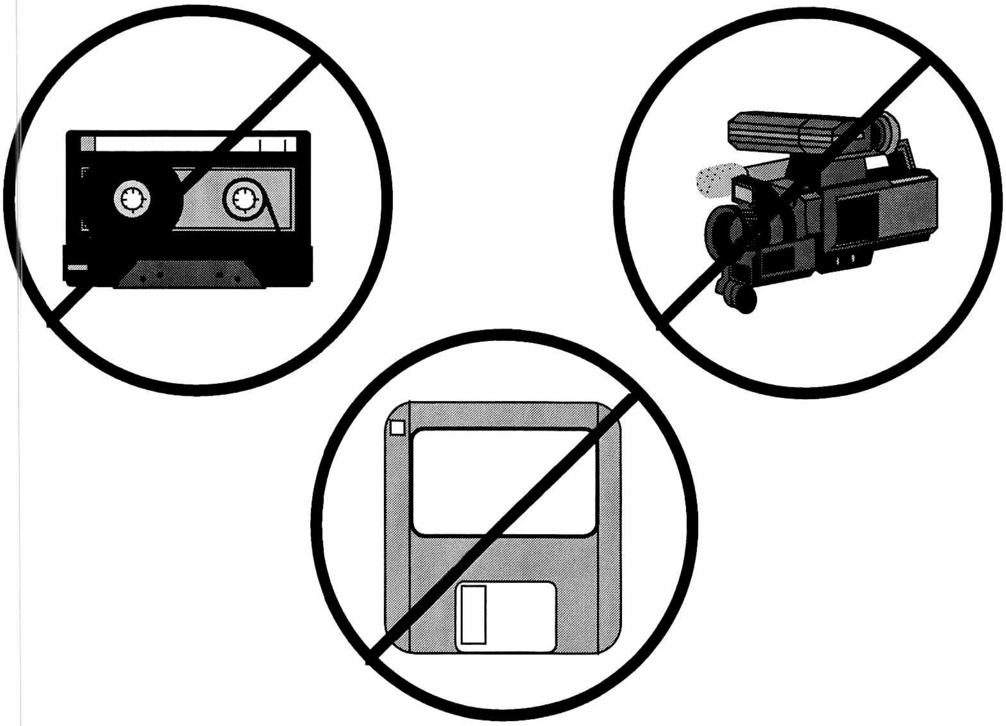
EMERGENCY INFORMATION

QUESTIONS

If you need to leave the room during the lecture portion of the course, please feel free to do so.

If you need to stand up in the back of the room, please feel free to do so.

Feel free to ask questions and share war stories!



Thank You!

SNIFFER® UNIVERSITY

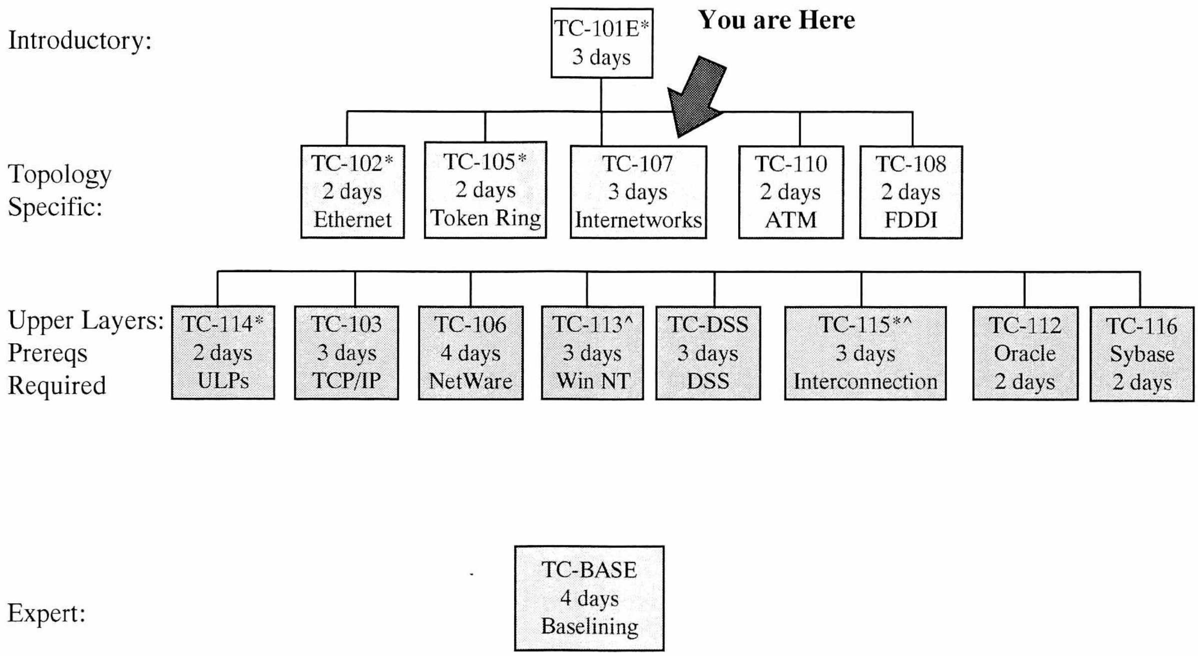
Overview 1 - 4
Internetwork Analysis and Troubleshooting, 10/96 Rev 5.0

It is a copyright violation to copy any files from the classroom equipment. Trace files are available on CD. An order form is available if the CD is not included in your manual.

Table of Contents

Course Overview

Curriculum Flowchart



SNIFFER® UNIVERSITY

Overview 1 - 7
Internetwork Analysis and Troubleshooting, 10/96 Rev 5.0

Network General

* These courses teach concepts that are required to pass the CNX test.

^ These courses are in development.

Objectives

Upon completion of this course you will:

- Possess the insight and skills to manage and troubleshoot LAN/WAN internetworks, using the Network General Corporation Sniffer Internetwork Analyzer.
- Understand the details of current and emerging technologies for interconnecting LANs.
- Use new knowledge and skills to troubleshoot WAN problems using the Network General Corporation LM2000 Analyzer.

Prerequisites:

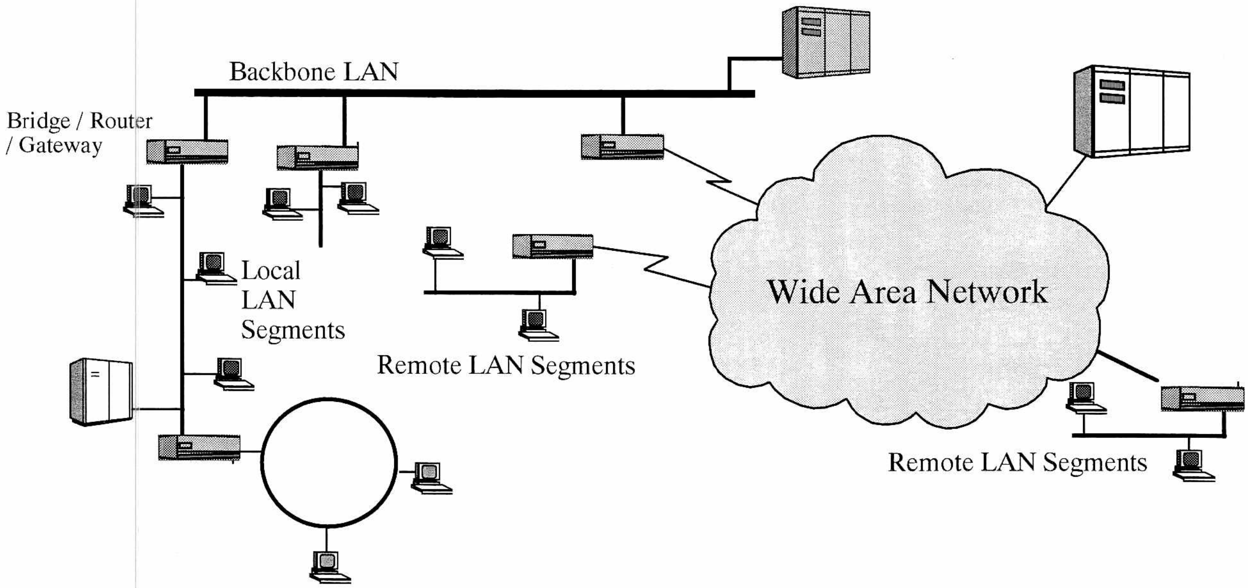
- LAN knowledge and experience using the Sniffer analyzer.
- Troubleshooting with the Sniffer Network Analyzer (**TC-101E**).

The LM2000 Analyzer is not available with Network General's Distributed Sniffer System.

Major Topics

- Overview of WAN Technology
- Product Overview and Interface Installation
- Sniffer Internetwork Analyzer
- T-1 Networking
- HDLC and related protocols
- Frame Relay
- PPP
- ISDN Fundamentals and Troubleshooting
- X.25

What is an Internetwork?



An internetwork is two or more geographically dispersed LANs interconnected over a wide area circuit, to share information and resources.

ISO-OSI Network Model

Layer	Function
7. Application	Access to the OSI environment for users and also provides distributed information services.
6. Presentation	Provides data representation (Syntax) independence to the application process.
5. Session	Provides the control structure for communication between applications. Establishes, manages and terminates connections (sessions) between applications.
4. Transport	Provides reliable, transparent transfer of data between end points. Provides end-to-end error recovery and flow control.
3. Network	Provides upper-layers with independence from the data transmission and switching technology used to connect systems. Concerned with routing packets, congestion control, fragmentation and reassembly.
2. Data Link	Provides for the reliable transfer of information across the physical link. Sends blocks of data (frames) in the proper format, along with the necessary synchronization, error control, and flow control.
1. Physical	Concerned with transmission of unstructured bit stream over physical medium; deals with the mechanical, electrical, functional and procedural characteristics to access the physical medium.

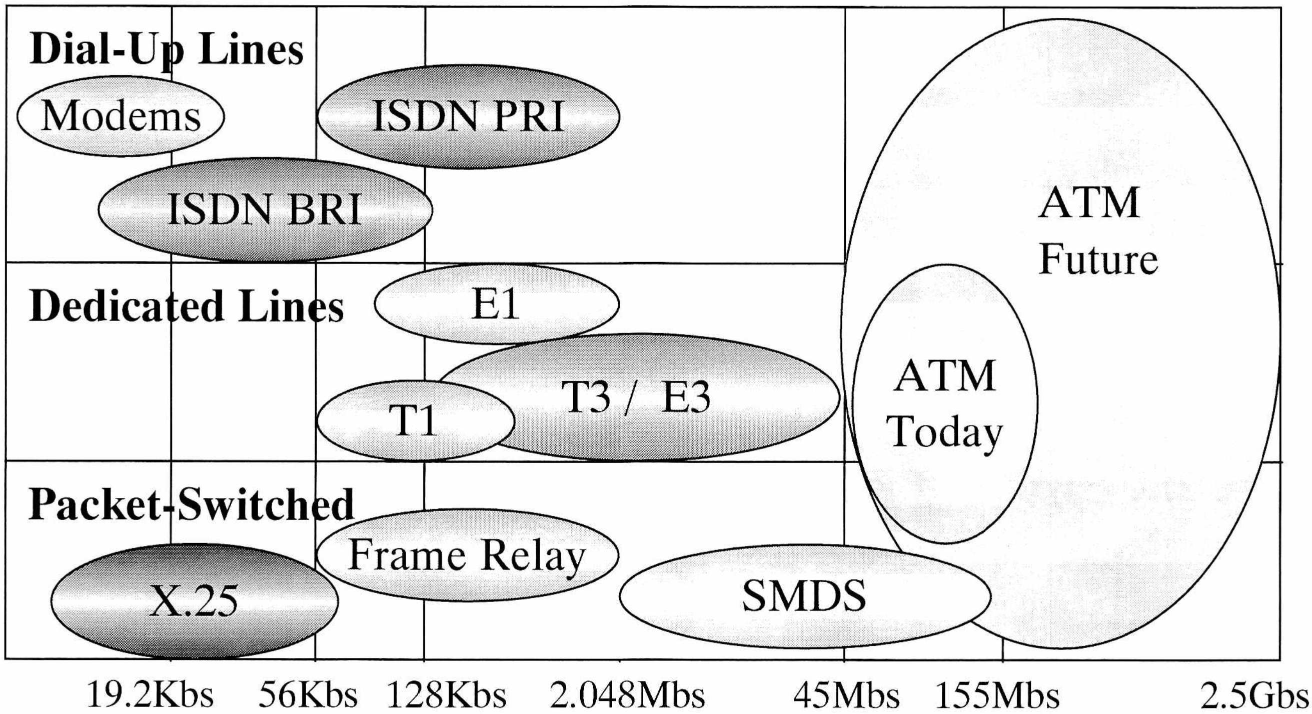
This is provided for your reference.

Common Problems Listed by Layer

Layer	Problems
7. Application	Slow response times, path searches, rights, file locking, file transfer throughput. Software logical flaws, virtual terminal, electronic mail, and other application problems.
6. Presentation	Data format, data conversion (i.e. ASCII to EBCDIC), terminal type conversion. Cryptography, data compression.
5. Session	Connection/Disconnection to Service Access Points. Problems can happen in three phases: connect, data transfer, release. Block size negotiation. Synchronization/resynchronization of sessions.
4. Transport	Multiplexing errors, multiple acknowledgments. Flow control overflows or time-outs, end-to-end connection terminations.
3. Network	Routing problems, packet splitting/reassemble errors, bottlenecks through networks links, routers, and gateways. Packet throughput and size limitations, allocation of network resources.
2. Data Link	Low level transmission quality problems, CRC errors, excessive collisions. Duplicate frames due to line errors.
1. Physical	Physical cable plant difficulties, opens/shorts, bad transceivers or repeaters. Radio frequency interference (RFI), Electromagnetic interference (EMI).

This is provided for your reference.

The Broadband World



Overview of WAN Technology

SNIFFER® UNIVERSITY

WAN Technology 2 - 1

Internetwork Analysis and Troubleshooting, 10/96, Rev 5.0

Network General

Objectives

On completion of this chapter you will:

- Know the types of Wide Area Circuits.
- Understand the differences between switching methods.
- Be able to classify the multiplexing methods.
- Recognize when a device is acting as a DTE or a DCE.

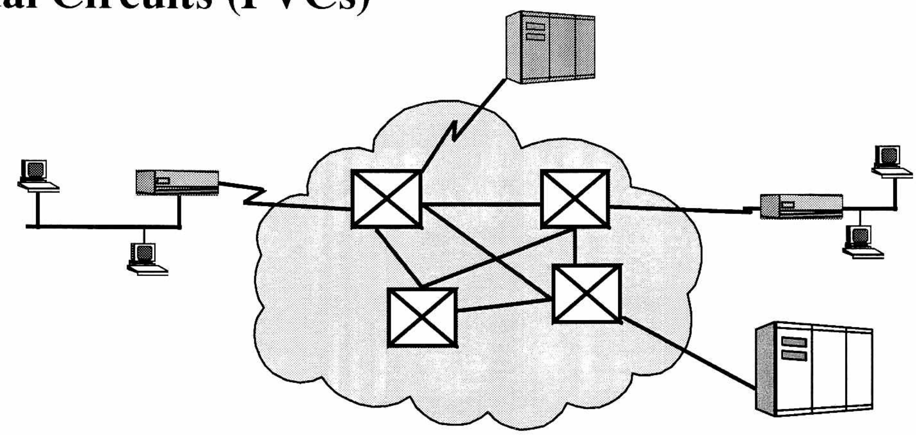
Model of WAN Technologies

OSI Model	WAN Protocols
Upper-layers	Data
Network layer	X.25; ISDN
Data Link layer	HDLC; Frame Relay; PPP; LAPB; LAPD
Physical layer	V.35; RS-232/V.24; RS-449; V.10/11; T1; E1; Fractional T1

We will be discussing these various WAN technologies. You may want to use this page for reference as we proceed through the course.

Types of Wide Area Circuits

- **Switched Virtual Circuits (SVCs) and Permanent Virtual Circuits (PVCs)**



- **Point-to-Point Circuits**

SNIFFER® UNIVERSITY

WAN Technology 2 - 4

Internetwork Analysis and Troubleshooting, 10/96, Rev 5.0

Network General

SVCs and PVCs are services provided within a Packet Switched Network (for example: X.25, Frame Relay).

An SVC is a logical connection that is maintained only for the duration of the call. Call setup and teardown packets are exchanged.

A PVC does not require call setup and teardown procedures, because a connection is permanently allocated between the end devices.

A point-to-point circuit is a fixed connection between two devices. It is typically provided by the phone company as a physical link only, with no protocol specified for packet transmission and reception.

Permanent Virtual Circuit

- PVC has only a single phase: data transfer.
- PVC is analogous to a leased line in a telephone network.
- PVC requires no call setup or clearing procedures.
- PVC has faster setup time.

Frame Relay was initially defined as a permanent connection protocol. A connection between two users is permanently established that cannot be cleared down at any time.

This mode of operation is referred to as Permanent Virtual Circuit (PVC), and is reasonably restrictive because users are not able to place frame relay connections to other users on demand. The connection will be setup (by a network manager) when the network starts up, and will permanently available until the network itself shuts down.

When a transmitting DTE sends a packet to the network, the identifying logical channel number in the packet indicates that the requesting DTE has a permanent virtual circuit connection to the receiving DTE. Services will now be provided without further session negotiation. PVC requires no call setup or clearing procedures, and the logical channel is continuously in a data-transfer state.

Switched Virtual Circuit

- SVC uses telephone dial up lines.
- SVC setup time slower.
- SVC's require three phases:
  - Call Setup
  - Data Transfer
  - Call Disconnection

Call Setup
The calling DTE issues a packet called a call request to the network, with a logical channel number and the address of the called DTE. The network uses the address to route the call request to the DCE that is to support the call at the remote end. This DCE sends an incoming call packet to the proper DTE. If the receiving DTE chooses to acknowledge and accept the call request, it transmits a call accepted packet to the network. The network transports this packet to the requesting DTE in the form of a call connected packet.
Data Transfer
The channel enters a data transfer state.
Call Disconnection
A clear request packet is sent by either end.
It is received as a clear indication packet.
The receiver confirms the disconnect by sending a clear confirm packet.
MCI marketing now claims that Frame Relay SVC is available.

Types of Switching in Networks

- **Circuit Switching** - a temporary dedicated connection, established and maintained for the duration of the call. Examples are a dial-up line and ISDN.

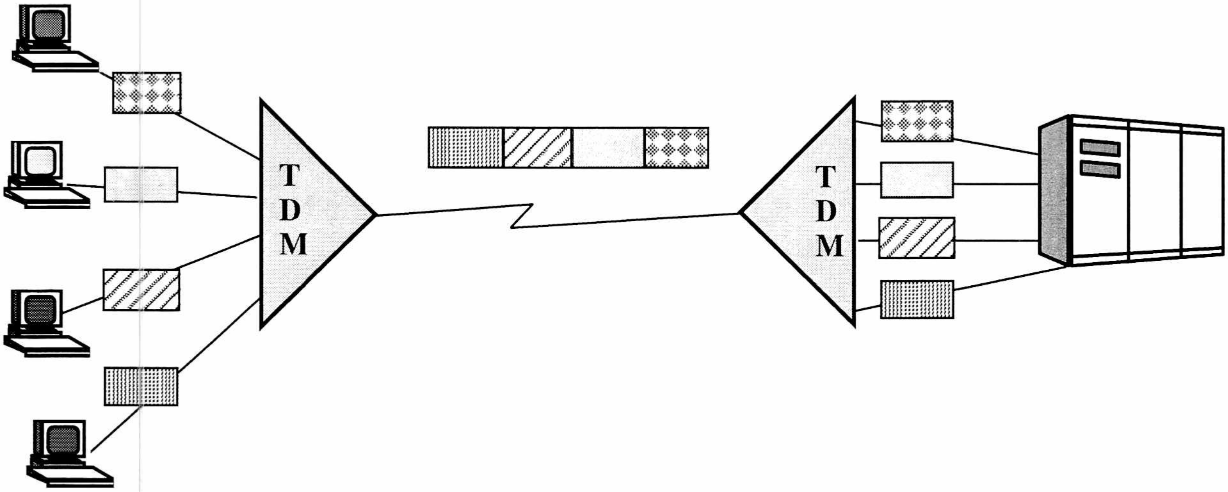
- **Packet Switching** - a shared circuit, where data is divided into packets which contain a unique identification and destination address. Examples are X.25, frame relay, ATM, and SMDS.

- **Message Switching** - designed for data traffic. The end users do not have a direct connection to one another. Instead, the message is transmitted to a message switch and is stored for future retrieval. An example is a mail server.

In packet switching networks, packets may go through different routes to reach their destination and arrive in a different order. The identification allows reassembly in the proper sequence.

ISDN uses both circuit switching and packet switching.

Time Division Multiplexing

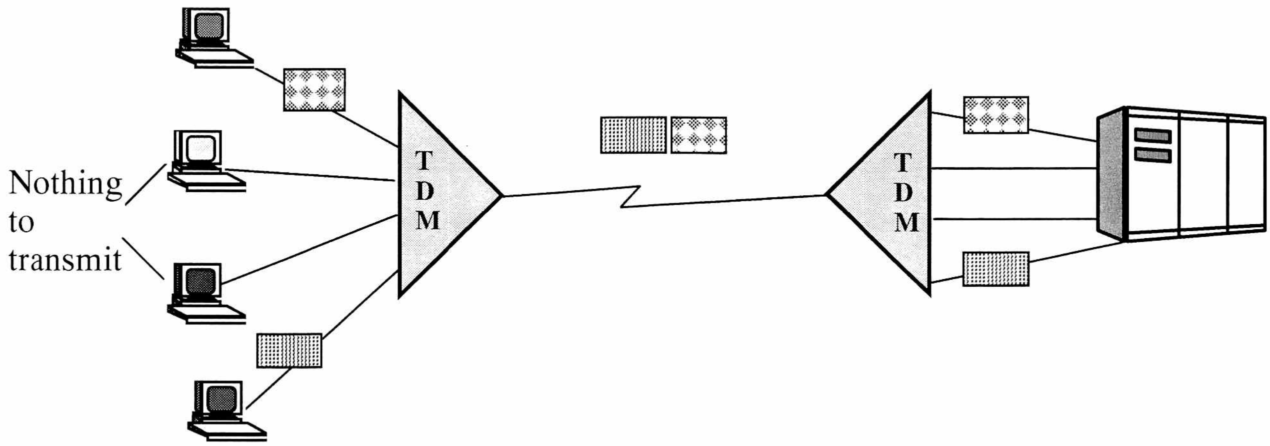


Time division multiplexing (TDM) is a method used to consolidate multiple slower lines into a single bit stream for transmission over a higher speed aggregate. Sequentially, a TDM-based multiplexer polls each input channel and devotes a unique "time slot" on the composite link for each device. If the device doesn't have any data to send, that portion of the bandwidth goes unused. Empty time slots are stuffed with bits/bytes as necessary to maintain the position of each station in the frame.

With TDM, the aggregate input speed cannot exceed the composite link speed.

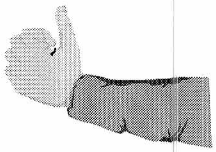
A mux must be on the receiving end to demultiplex the individual time slots, and forward them to the appropriate channel.

Statistical Time Division Multiplexing

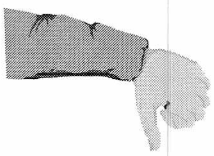


- STDM works like TDM, except that when no data is present on an input channel, the available bandwidth is usable by a station that is ready to send data.
- STDM is useful for burst-oriented data, where not all devices will be operating at peak channel capacity at the same time.
- With STDM, the aggregate peak input speed can be exceeded, because the mux uses a buffer to hold data until bandwidth becomes available.
- Inverse multiplexing is a fairly new technique, whereby multiple links become available on demand.
- Proprietary stat muxes must use same vendor solution at each end.

Advantages and Disadvantages of STDM



- Efficiency of bandwidth.
- Port contention: allows a larger number of stations to contend for a lesser number of channels.
- Channel prioritization- can be configured to poll any given channel more often.



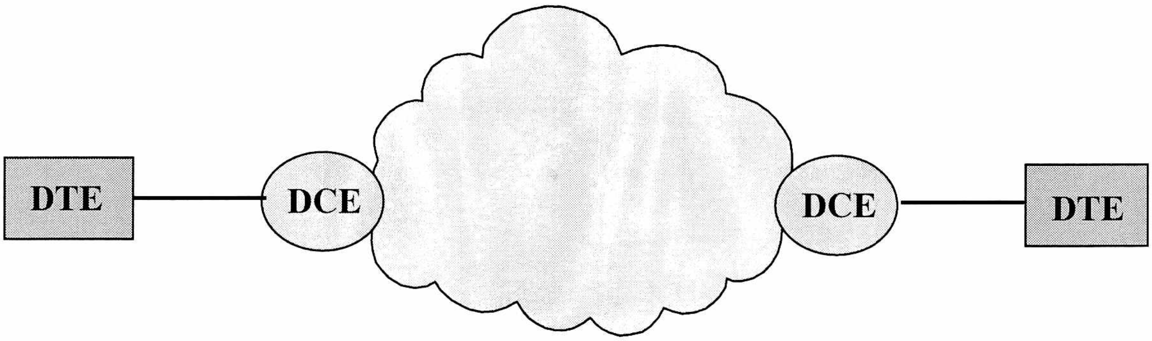
- Processing intensive so transmission speeds not as fast as TDMs.
- More costly than TDMs.

SNIFFER® UNIVERSITY

WAN Technology 2 - 10
Internetwork Analysis and Troubleshooting, 10/96, Rev 5.0

- Voice and video are provided by some vendors.
- The main problem with voice and video applications is the delay factor

DTE and DCE



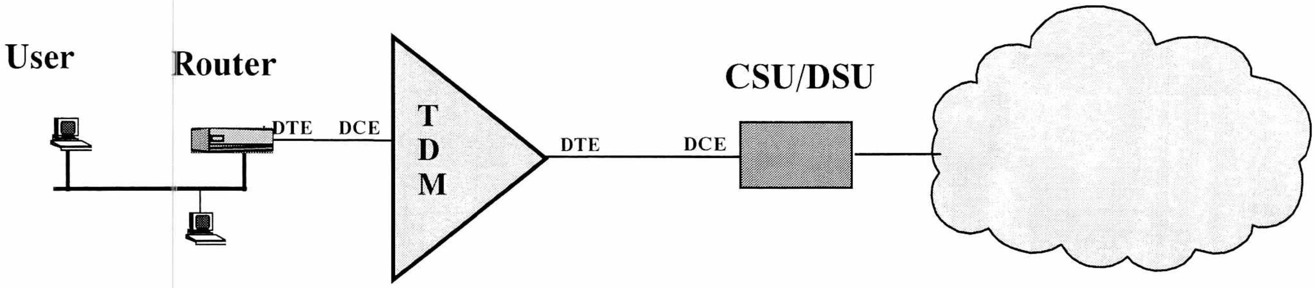
Historically, DTE, which stands for **Data Terminal Equipment**, has been the end user device - terminal, mini, or mainframe. DCE, which stands for **Data Circuit Terminating Equipment** or more recently **Data Communications Equipment**, has provided the interface to the cloud.

When RS-232 WAN circuits were state of the art, determining the DTE and DCE was easy. A DTE transmitted on pin 2 and a DCE transmitted on pin 3.

DTE (Data Terminal Equipment) is a general term used to refer to the device a user interfaces with. It is usually a terminal or computer. The DTE runs user applications.

DCE (Data Communications Equipment) connects a DTE to the communications channel. It is generally separate from the DTE and the media, though it doesn't need to be (e.g. Router with built in CSU/DSU). The DCE's primary function is to convert the DTE's data format to a signal suitable for the media. A modem is one example of a DCE.

DTE and DCE and DTE and DCE?

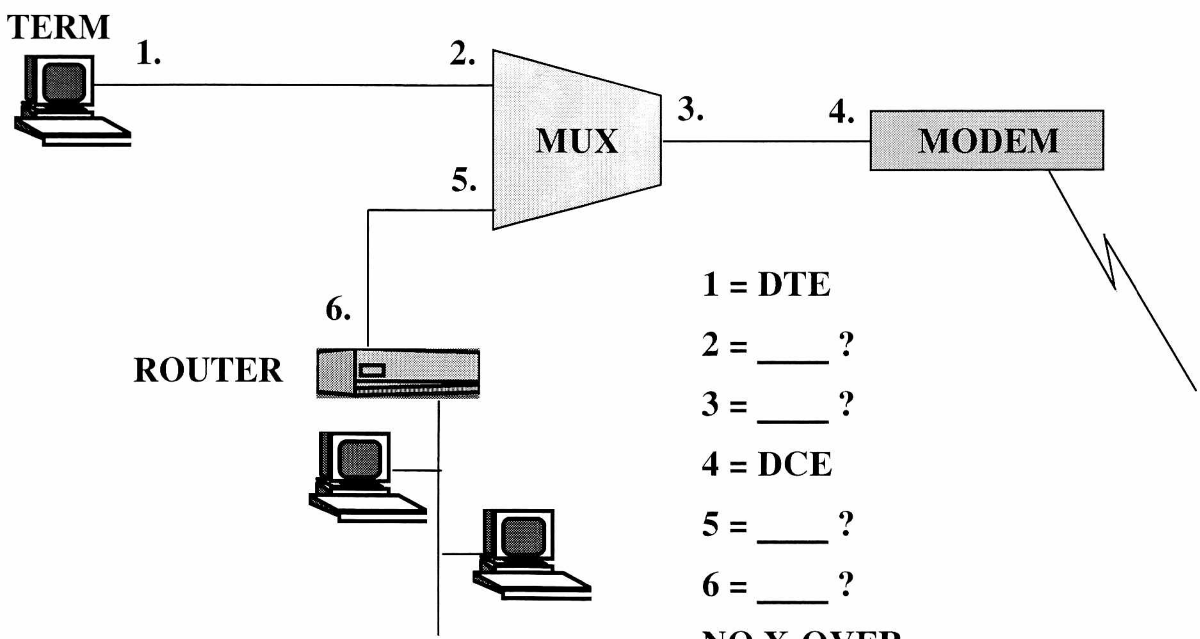


The complexity of modern networking has somewhat expanded the concept of DTE and DCE. Today, it's important to think of DTE and DCE in a much broader sense. The DTE provides services to the user, and the DCE interfaces the DTE to the wide area network, usually referred to as simply the network.

In an enterprise-wide network, a user on an Ethernet segment will be connected to a router, which may be an input to a TDM, which may or may not have a built-in CSU/DSU! Which one is the DTE and which one is the DCE? The router would be the DTE and the TDM would be the DCE. If the TDM interfaced to CSU/DSU, then the TDM would be the DTE and the CSU/DSU the DCE.

Later when we analyze traffic captured with the Sniffer Internetwork Analyzer (SIA), we will see sessions between the DTE and the DCE. Since the SIA attaches between a bridge/router and a DSU/CSU, the bridge/router and CSU/DSU are the physical DTE and DCE, but the broader concept of user and network still applies.

DTE vs DCE



1 = DTE

2 = ____ ?

3 = ____ ?

4 = DCE

5 = ____ ?

6 = ____ ?

NO X-OVER

The DTE is the source, the sink, or both in the system. It transmits and/or receives data by utilizing the DCE and transmission channel. Don't be misled by the name "data terminal equipment"; these could be any device that can transmit or receive data.

The DCE and transmission channel perform the function of moving the data from one point to another. In general, they neither know nor care about the content of the information transmitted.

When determining whether the equipment is acting as a DTE or DCE, you need to consider where the analyzer is attached.

Summary

- There are Switched and Permanent Virtual or PPP Circuits.
- Wide Area switches can use circuit, packet or message switching.
- Circuits can be multiplexed, using either time or statistical time division.
- DCEs interface the user devices (DTEs) into the Wide Area network.

Product Overview

Objectives

On completion of this section you will be able to:

- Explain the features of the Sniffer Internetwork Analyzer (SIA).
- Summarize the interface options and features of the Line Interface Card.
- Use the LM2000 Analyzer to test your Line Interface Card.
- Differentiate the characteristics of the various interface cables.
- Install the T1/E1 pod to monitor or test the channels in a T1/E1 circuit.

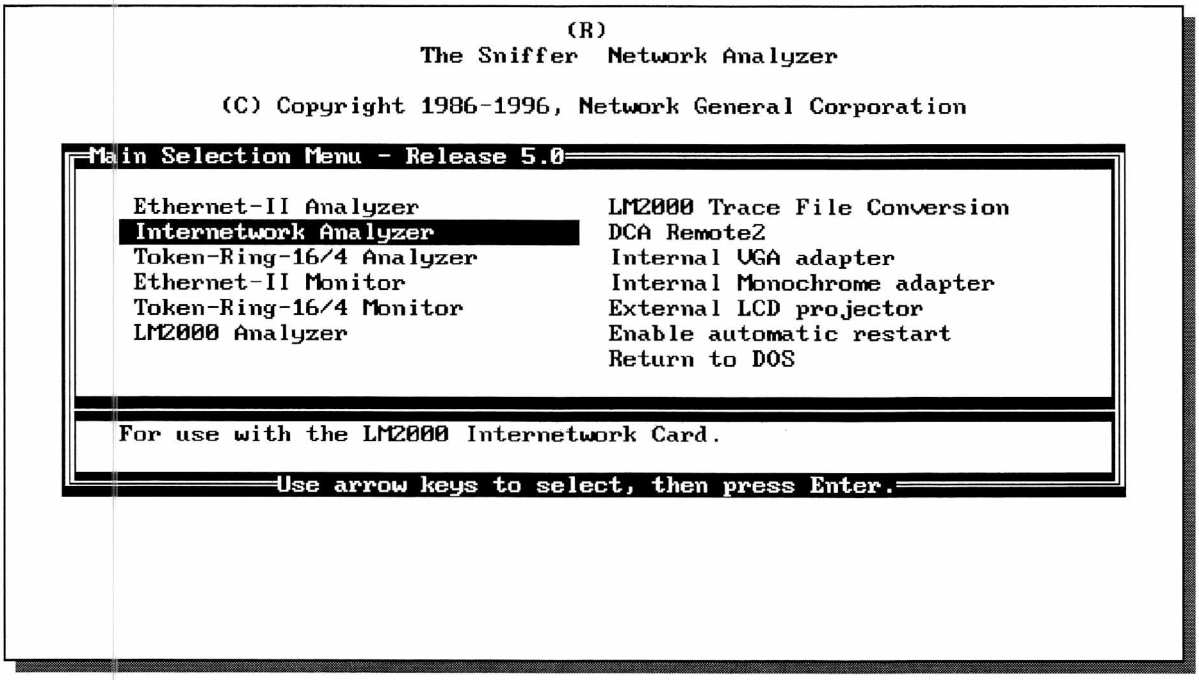
Product Overview

- The Sniffer Internetwork Analyzer (SIA) provides expert analysis for WAN/Synchronous internetworks.
- Captures data up to T1 (1.544 Mbps), E1 speeds (2.048 Mbps) or ISDN (B & D channels).
- Helps maintain, troubleshoot, fine-tune, and expand your network or internetwork.
- Analyzes over 140 LAN protocols encapsulated within various WAN frame formats.
- LM2000 provides BERT, BLERT and physical interface testing to enhance WAN analysis.

BERT- Bit Error Rate Test

BLERT- Block Error Rate Test

The Main Selection Menu



SNIFFER® UNIVERSITY

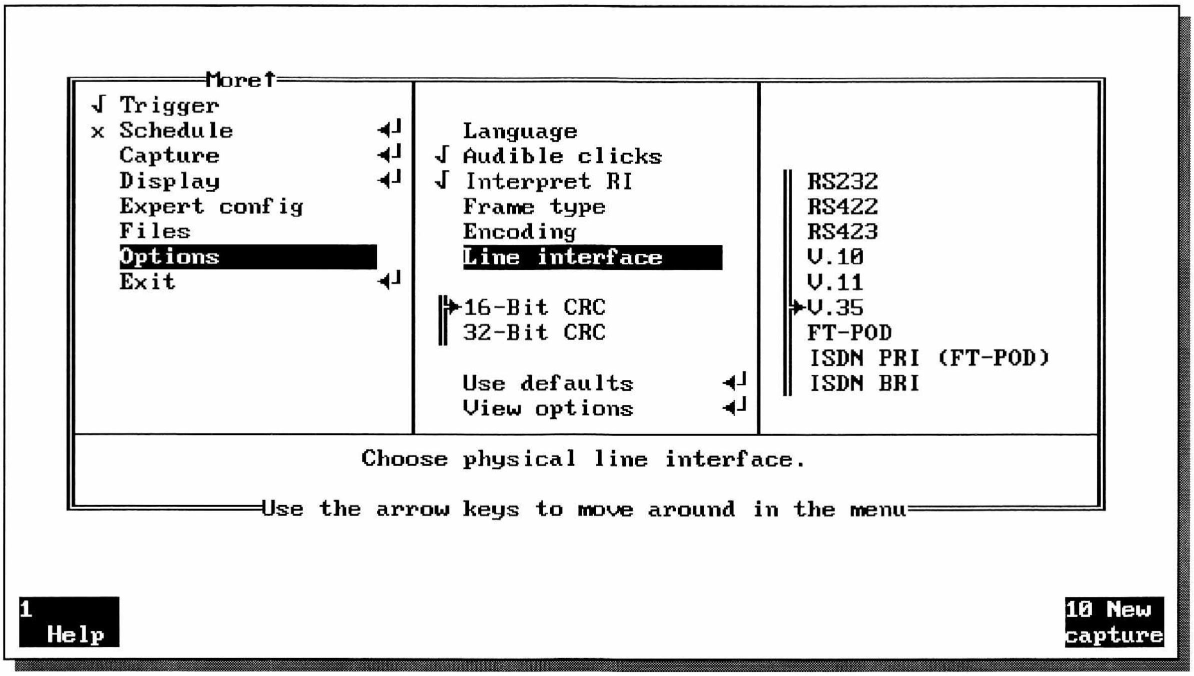
Product Overview 3 - 4
Internetwork Analysis and Troubleshooting, 10/96 Rev. 5.0

Network General

Three applications are bundled with the SIA: the Sniffer Internetwork Analyzer, the LM2000 Analyzer, and the LM2000 Trace File Conversion utility.

- The SIA provides seven layer protocol analysis.
- The LM2000 provides BERT (bit error rate testing), a software based break-out box, asynchronous terminal emulations, and up to layer 3 protocol analysis.
- The LM2000 Trace File Conversion utility converts trace files **between** the SIA format and LM2000 format.

Line Interface Options



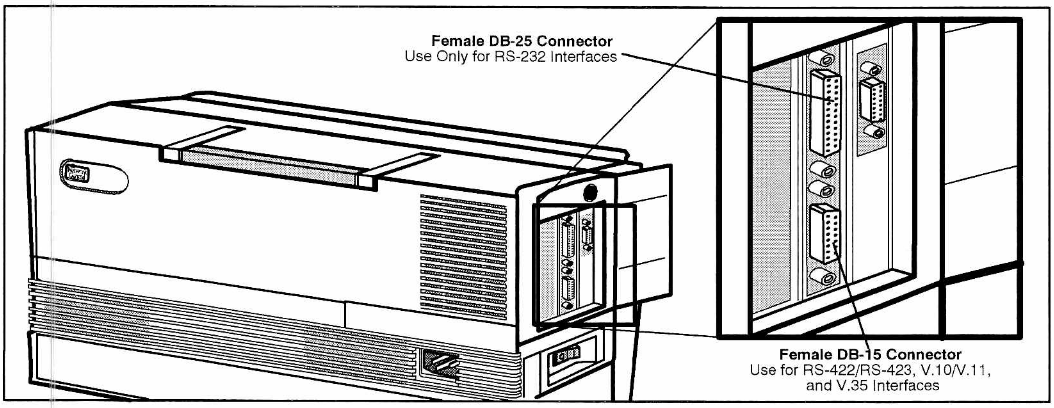
SNIFFER® UNIVERSITY

Product Overview 3 - 5

Internetwork Analysis and Troubleshooting, 10/96 Rev. 5.0

** Remember, selecting the wrong interface can bring down your network **

The Line Interface Card



The top connector on the line interface card is a 25-pin, D-type connector (DB-25) and is used **only** for RS-232 network devices. The lower connector is a 15-pin, D-type connector (DB-15) and is used for RS-422 and RS-423 (RS-449), V.10/V.11, and V.35 installations.

Caution: the DB-15 connector used for the high speed WAN card is physically identical to the DB-15 AUI connector on an Ethernet adapter. Use care to insert the WAN Y-cable into the appropriate connector on the high speed WAN card.

Interface Options

- The Sniffer Internetwork Analyzer supports the following physical line interfaces:
  - RS-232
  - RS-422
  - RS-423
  - V.10
  - V.11
  - V.35
- All connections between the Sniffer Internetwork Analyzer (SIA) and the network are made using one of two connectors on the line interface card.

RS-232	25 pin DTE/DCE interface. Uses SIA 25 pin connector.
RS-422	Balanced signaling for data rates from 100K to 10Mbps. Uses SIA 15 pin connector.
RS-423	Unbalanced signaling for data rates from 1K to 100Kbps. Uses SIA 15 pin connector.
V.10	CCITT (European) equivalent of RS-423. Uses SIA 15 pin connector (unbalanced).
V.11	CCITT (European) equivalent of RS-422. Uses SIA 15 pin connector (balanced).
V.35	Interface to 56K and T-1 (1.544Mbps) circuits. Uses SIA 15 pin connector.

Standards for the DTE/DCE Interface

The Standards are broken into four areas:

- The **mechanical** characteristics for the interface
- The **electrical** signals across the interface
- The **function** of each of the electrical signals across the interface
- The **procedures** for certain applications

The **mechanical** characteristics are the actual physical interface between the DTE and DCE (e.g. cable length connector type, and pin location).

The **electrical** specification of the standard defines the voltage and current for each pin. It also determines the signaling between the DTE and DCE and the voltage to be used.

The **functional** specification details which circuits (RTS, CTS, etc.) are connected to each of the pins in the interface. The standard supports one data circuit in each direction; therefore full duplex is possible. Functions can be classified into four general areas related to data, ground, timing, and control.

The **procedural** spec covers the sequencing of signals and actions taken by the DTE and DCE. For example, a Request to Send from the DTE normally receives a Clear to Send response from the DCE.

DTE to DCE Standards

TYPE	PINS	ELECTRICAL	MECHANICAL	FUNCTIONAL
Low and medium speed, unbalanced	25	EIA RS-232-C	ISO 2110	EIA RS-232-C
	25	EIA-232-D	EIA-232-D	EIA-232-D
	25	MIL-188-C	MIL-188-C	MIL-188-C
	25	CCITT V.28	ISO 2110	CCITT V.24
	37	EIA-RS-423	ISO 4902	EIA RS-449
	37	MIL-188-114	MIL-188-114	MIL-188-114
	15	CCITT V.10	ISO 4903	CCITT X.24
High speed, balanced	25	EIA 530	EIA 530	EIA 530
	37	EIA RS-422	ISO 4902	EIA RS-449
	37	MIL-188-114	MIL-188-114	MIL-188-114
	34	CCITT V.35	ISO 2593	CCITT V.35
	15	CCITT V.11	ISO 4903	CCITT X.24

RS-232 Adapter Cable Wiring

DB-25 Pin	Lead	Function	RS-232 Circuit	V.24 Circuit	DB-25 Pin	Lead	Function	RS-232 Circuit	V.24 Circuit
1	PG	Protective Ground	AA	101	11	EQ	Equali - zation	-	-
2	TD	Transmit Data	BA	103	15	TC	Transmit Clock	DB	114
3	RD	Receive Data	BB	104	17	RC	Receive Clock	DD	115
4	RTS	Request To Send	CA	105	20	DTR	Data Terminal Ready	CD	108.2
5	CTS	Clear To Send	CB	106	22	RI	Ring Indicator	CE	125
6	DSR	Data Set Ready	CC	107	24	EXTC	External Clock	DA	113
7	SG	Signal Ground	AB	102	25	BUSY	Busy	-	-
8	DCD	Data Carrier Detect	CF	109	-	-	-	-	-

These pinouts are included for your reference.

Electrical spec, also called V.28 and MIL-188.
The International version of RS-232's physical layer spec is CCITT's V.24.
Both specify:

- A maximum cable length of 50 feet.
- Most commonly uses DB 25 pin mechanical connector.
- It employs unbalanced signaling.
- Maximum data rate: 20 Kb/s.
- Version C is the most popular, version D adds loopcode support.

V.35 Adapter Cable Wiring

Function	Lead	V.35 Pin	DB-15 Pin	Function	Lead	V.35 Pin	DB-15 Pin
Transmit Data	TD (A) (B)	P S	2 9	Transmit Timing	TC (A) (B)	Y AA	6 13
Receive Data	RD (A) (B)	R T	4 11	Receive Timing	RC (A) (B)	V X	7 14
Request To Send	RTS	C	3	Ring Indicator	RI	J	15
Data Terminal Ready	DTR	H	10	Receive Line Signal Detect	RLSD	F	8
Clear To Send	CTS	D	5	Ground	GND	A,B	1
Data Set Ready	DSR	E	12	-	-	-	-

These pinouts are included for your reference.

CCITT V.35 is the international standard termed “Data Transmission at 48 Kbps Using 60-108 KHz Group-Band Circuits”. It is typically used for DTE or DCE that interface to high speed digital carrier, such as DDS.

High speed interface - up to 10 Mb/s.
Uses a special 34 pin connector.
Used in U.S. for 56 Kb/s and faster.

RS530 is V.35 on RS232 connector.

V.10/V.11 Adapter Cable Wiring

Function	Lead	DB-15 Pin	Function	Lead	DB-15 Pin
Shield	N/A	1	I Indication	I (A) (B)	5 12
Transmit Data	T (A) (B)	2 9	S Signal Timing	S (A) (B)	6 13
Receive Data	R (A) (B)	4 11	G Ground	G	8
Control	C (A) (B)	3 10	-	-	-

These pinouts are included for your reference.
V.11/10 functional specs are identical to RS-422/423.

V.10 is unbalanced and V.11 is balanced.

Adapter Cable Wiring
RS-449 (RS-422/423)

Function	Lead	DB-37 Pin	DB-15 Pin	Function	Lead	DB-37 Pin	DB-15 Pin
Signal Ground	SG	19	1	Request To Send	RS (A) (B)	7 25	3 10
Send Data	SD (A) (B)	4 22	2 9	Receive Timing	RT (A) (B)	8 26	7 14
Receive Data	RD (A) (B)	6 24	4 11	Clear To Send	CS (A) (B)	9 27	5 12
Send Timing	ST (A) (B)	5 23	6 13	-	-	-	-

These pinouts are included for your reference.

RS-449 was originally intended to replace RS-232, but RS-232 and RS-449 are completely incompatible.
RS-449 permits greater cable distances, higher transmission speeds and more interchange circuits than RS-232.
RS-449 commonly uses DB-37 pin mechanical connector.
Two electrical specs exist for RS-449:
- RS-422: defines a balanced interface.
  - 10 Mb/s (up to 40 ft of cable)
  - 100 Kb/s (up to 4000 ft of cable)
- RS-423: defines a unbalanced interface.
  - 100 Kb/s (up to 40 ft of cable)
  - 1 Kb/s (up to 4000 ft of cable)

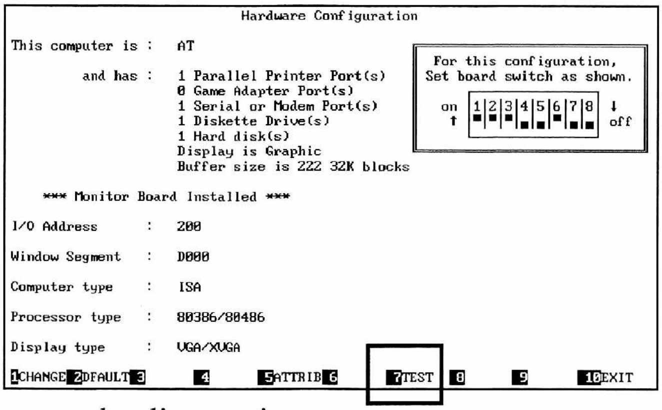
Diagnostics for the WAN/Synchronous Line Interface Card

- Because the Sniffer Internetwork Analyzer and the LM2000 share the same line interface card, you can use the diagnostics provided with the LM2000 to test the operation of the line interface card.
- Diagnostics confirm that the card is firmly seated in your PC and that the onboard memory and microprocessor are functioning correctly.

To run the hardware test on the Sniffer Internetwork Analyzer interface card...

Line Interface Card Lab

1. Start the LM2000 Analyzer from the Main Selection Menu by highlighting the LM2000 Analyzer menu entry and pressing **Enter**.
2. At the LM2000 Analyzer Main Menu, press **<Shift> F2** to access the Hardware Configuration Screen. This screen shows you the default switch settings for the line interface card. If you were experiencing installation problems, verify that the line interface card switch settings are set to the default.



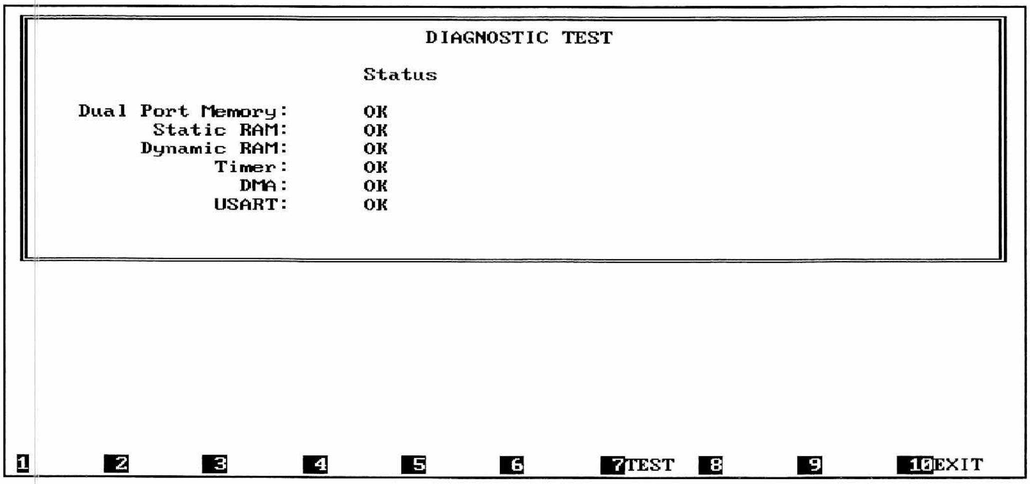
3. Press **F7 Test** to run the diagnostics.

If display is not set to graphics, you will not be able to display in color.

Line Interface Card Lab

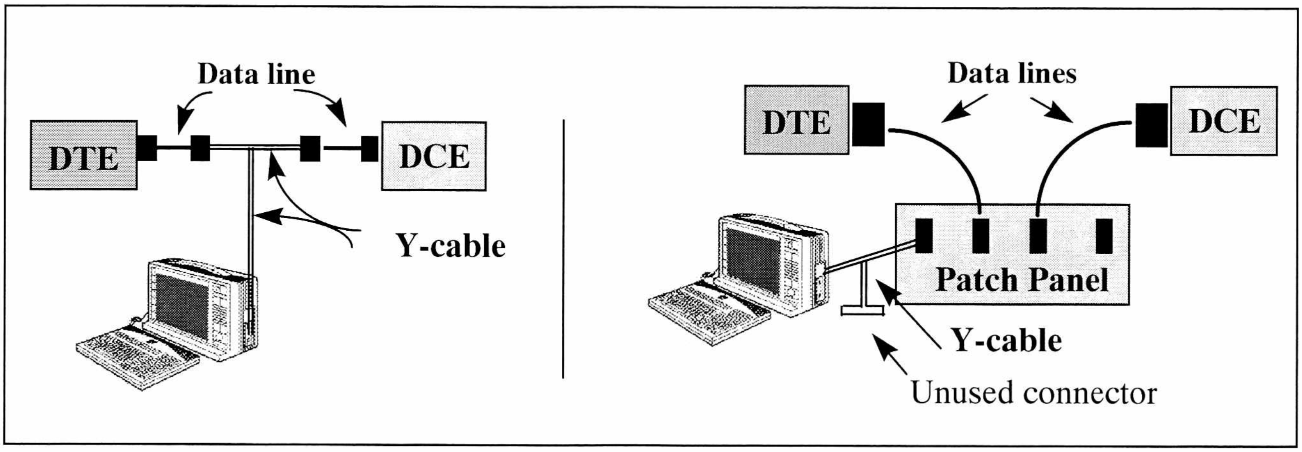
(Continued)

This screen will indicate which tests are successful and which have failed.



4. When the tests are complete (TEST reappears next to **F7**), press **F10 (Exit)** or **Esc** to return to the Hardware Configuration Screen.

Two Ways to Connect to the Network



Each Y-cable provides one female and two male connectors. The Y-cable provides two ways to connect the analyzer to the network: in-line or through a patch panel.

In this context, DTE (Data Terminal Equipment) usually refers to a bridge or router, and DCE (Data Communications Equipment) a CSU/DSU or modem.

The SIA is a passive device and derives its timing from the DCE. If after connecting to the network you see a "clock absent" message, check the cabling, card, etc.

A Word of Caution

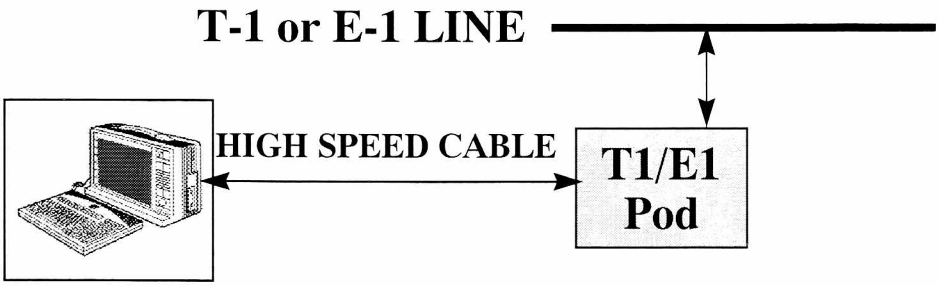
Before connecting the Sniffer Internetwork Analyzer to the data line in a non-patched mode:

- Verify that there is no traffic on the line.
- Notify the appropriate parties that the network will be down temporarily.
- Verify there is no traffic again.

Adapter Cables

- Four adapter cables provide the necessary wiring conversions between the network interface and the line interface card.
- The following cables are provided by default:
  - US. Customers: RS-232, V.35
  - Outside the U.S.: RS-232, V.35, V.10/V.11
  - Optional: RS-422/423

Network General Interface Pods



- The T-1 Pod is used for monitoring, or testing, from 1 to 24 channels of a T-1 circuit. (E1 is 1-32 channels.)
- The T-1 Pod can be operated either attached to the protocol analyzer or independently.
- When attaching to the SIA, the T-Pod always uses the DB-15 (high speed) connector.

There are several different PODS available: T1, E1, Fractional and even an ISDN version. Just make sure you have the correct POD for your environment.

The T-1 Pod

(Continued)

There are four test modes for the T-1 Pod:

- **Monitor** - Data monitored at RX1 is transmit data. Data monitored at RX2 is receive data. Data can be monitored over one or more DS0s. (This mode is normally used.)
- **Terminate** - Allows a protocol analyzer to monitor incoming data on RX1 while transmitting data on TX1.
- **Drop and Insert (D/I)** - Allows the protocol analyzer to access one or more DS0s, and replace the original data in them with its own data or test patterns. Any unselected channels are unaffected.
- **Log Test** - The T-1 Pod monitors for alarm conditions and prints these out at set intervals. In this mode, the T-1 Pod connects directly to a printer instead of the analyzer.

Note: All connections from the T-Pod to the SIA use the high speed connector (DB-15).

Summary

The Sniffer Internetwork Analyzer provides the following support:

- WAN Synchronous Line Interface card.
- RS232, RS422, RS423, V.10, V.11, V.35 and various Pod line interfaces.
- LM2000 Analyzer provides testing for the card.
- The SIA can be attached directly to the data line with a Y cable or the Y cable can be used to attach it to a patch panel.
- The pods attach to the high speed connector of the Line Interface card and enable the SIA to monitor a T1, E1, fractional, or ISDN circuit.

The Sniffer Internetwork Analyzer

SNIFFER® UNIVERSITY

SIA Overview 4 - 1

Internetwork Analysis and Troubleshooting, 10/96 Rev. 5.0

Network General

This section covers the differences between the SIA and LAN Expert Sniffer Analyzer.

Objectives

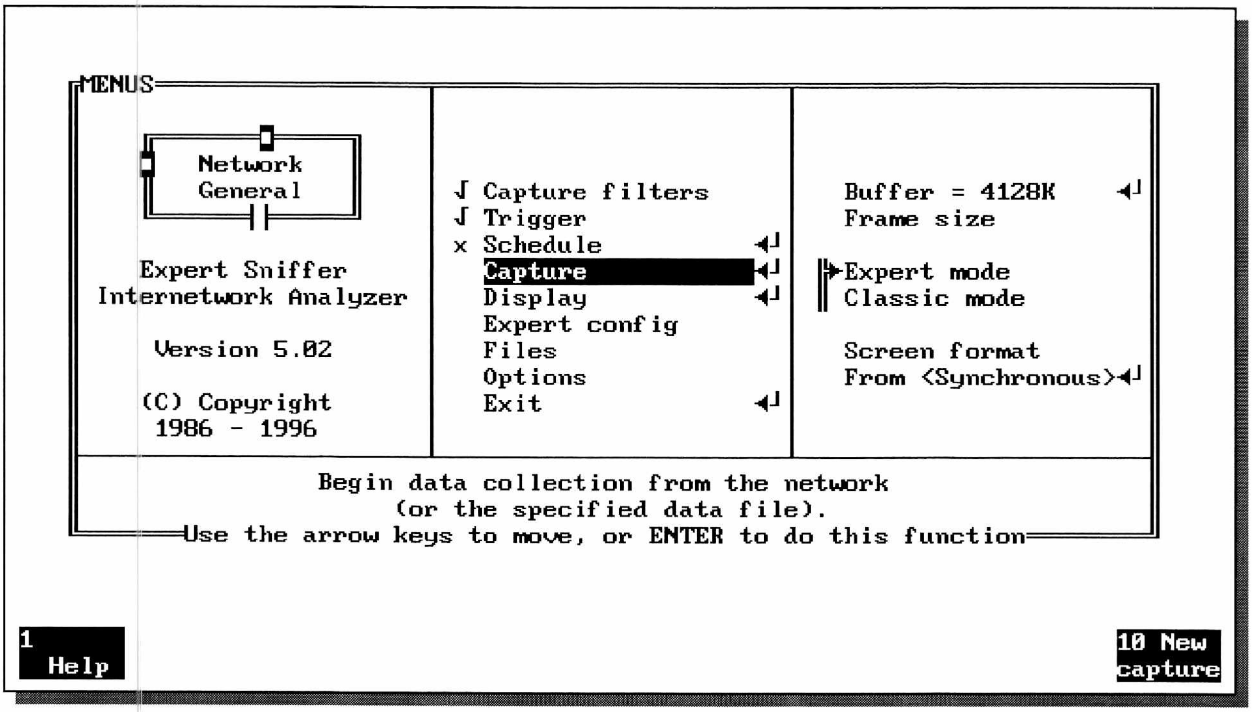
On completion of this chapter you will:

- Know how to use the features unique to the Sniffer Internetwork Analyzer (SIA).
- Recognize when and how to appropriately adjust the Expert thresholds.
- Be able to set up protocol forcing to enable the Sniffer Internetwork Analyzer to decode encapsulated protocols.
- Demonstrate how to troubleshoot and optimize WAN area connections using information provided by the SIA.

The Main Selection Menu

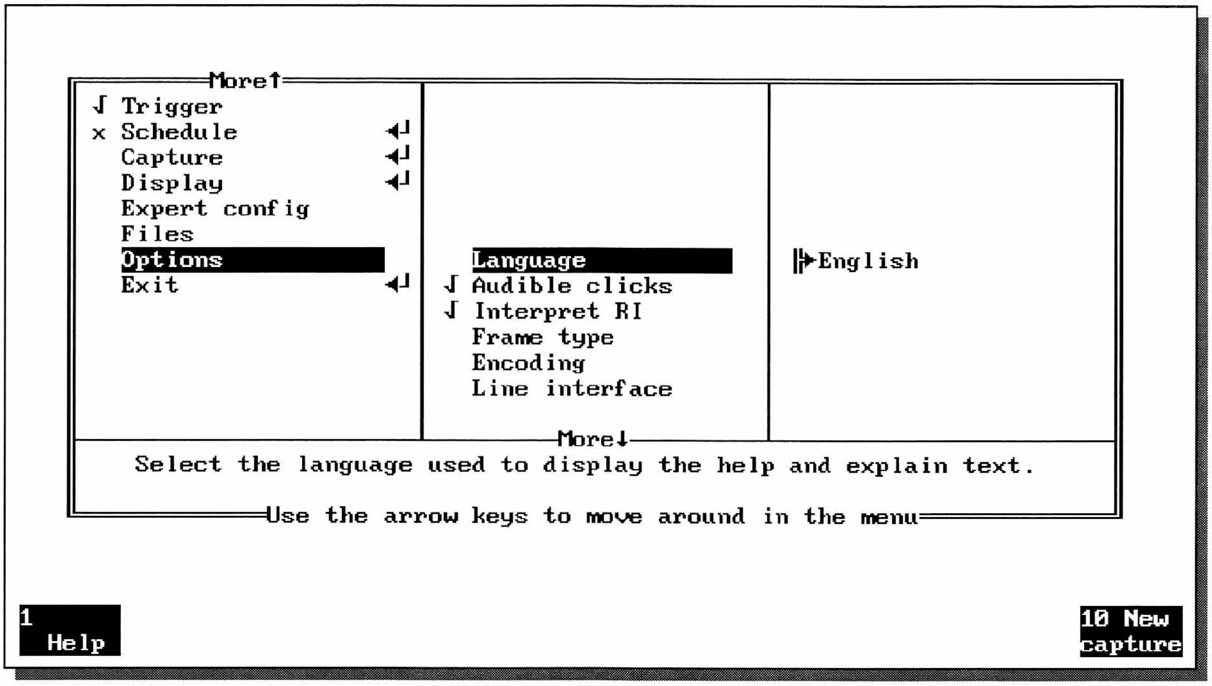
```
                              (R)
                The Sniffer  Network Analyzer

       (C) Copyright 1986-1996, Network General Corporation

 Main Selection Menu - Release 5.0

   Ethernet-II Analyzer           LM2000 Trace File Conversion
   Internetwork Analyzer          DCA Remote2
   Token-Ring-16/4 Analyzer       Internal VGA adapter
   Ethernet-II Monitor            Internal Monochrome adapter
   Token-Ring-16/4 Monitor        External LCD projector
   LM2000 Analyzer                Enable automatic restart
                                  Return to DOS

  For use with the LM2000 Internetwork Card.

             Use arrow keys to select, then press Enter.
```

The Main Menu



The user interface is the same as the Sniffer analyzer

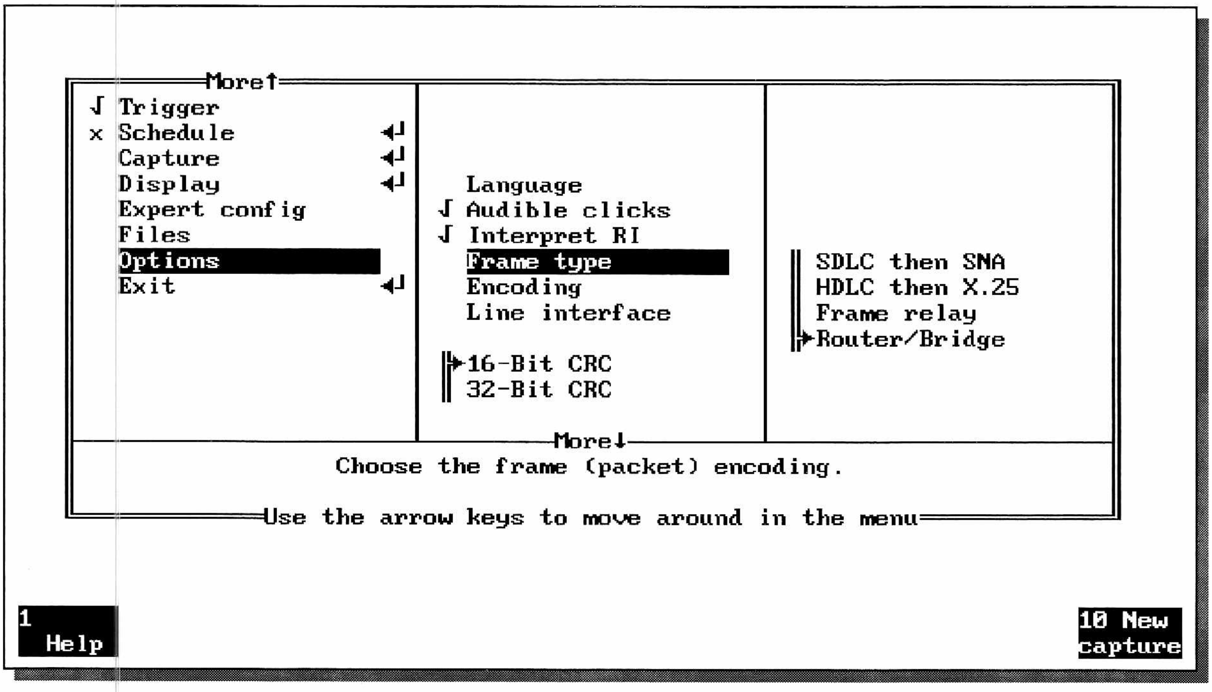
Options



The available language options are French, Italian, German, and English.

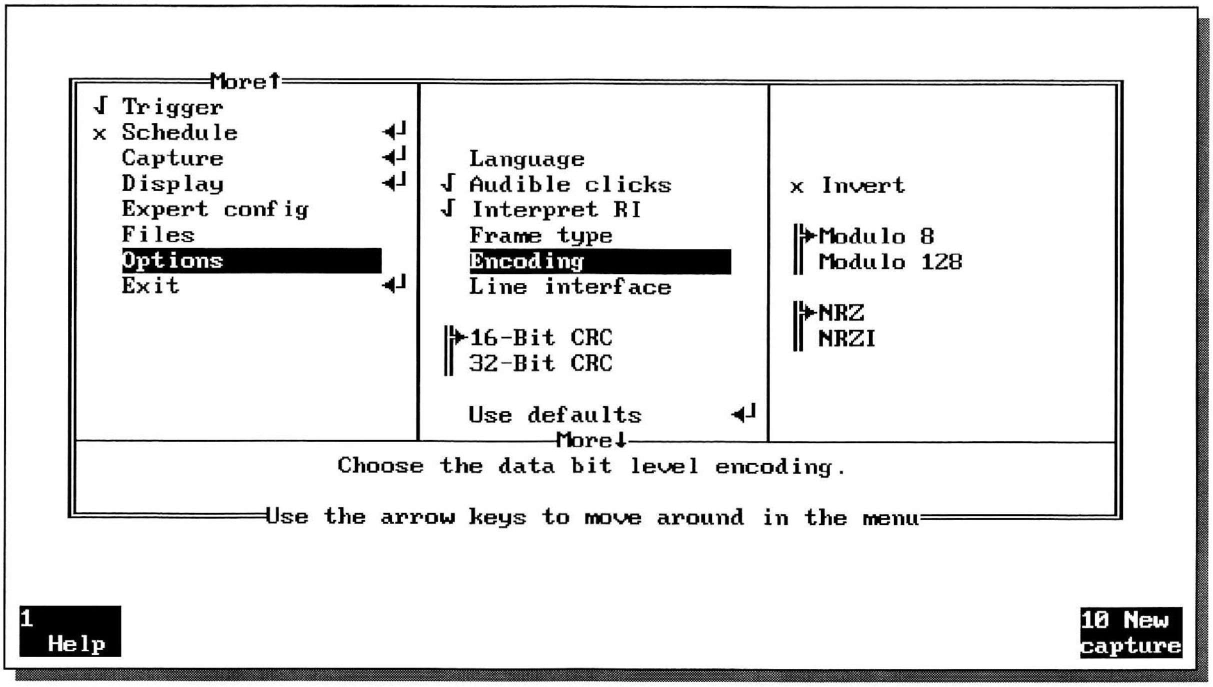
SIA Overview 4 - 5

Frame Type



The **Frame type** option lets you define the access protocol. Of these protocols, the most widely used are **SDLC then SNA** in IBM installations, and **HDLC then X.25**, which is widespread in Europe and is used increasingly in the US. The **Frame relay** type is primarily used for LAN interconnectivity over leased lines, as are proprietary versions of HDLC (decoded by the **Router/Bridge** option).

Encoding Options



SNIFFER® UNIVERSITY

SIA Overview 4 - 7
Internetwork Analysis and Troubleshooting, 10/96 Rev. 5.0

Network General

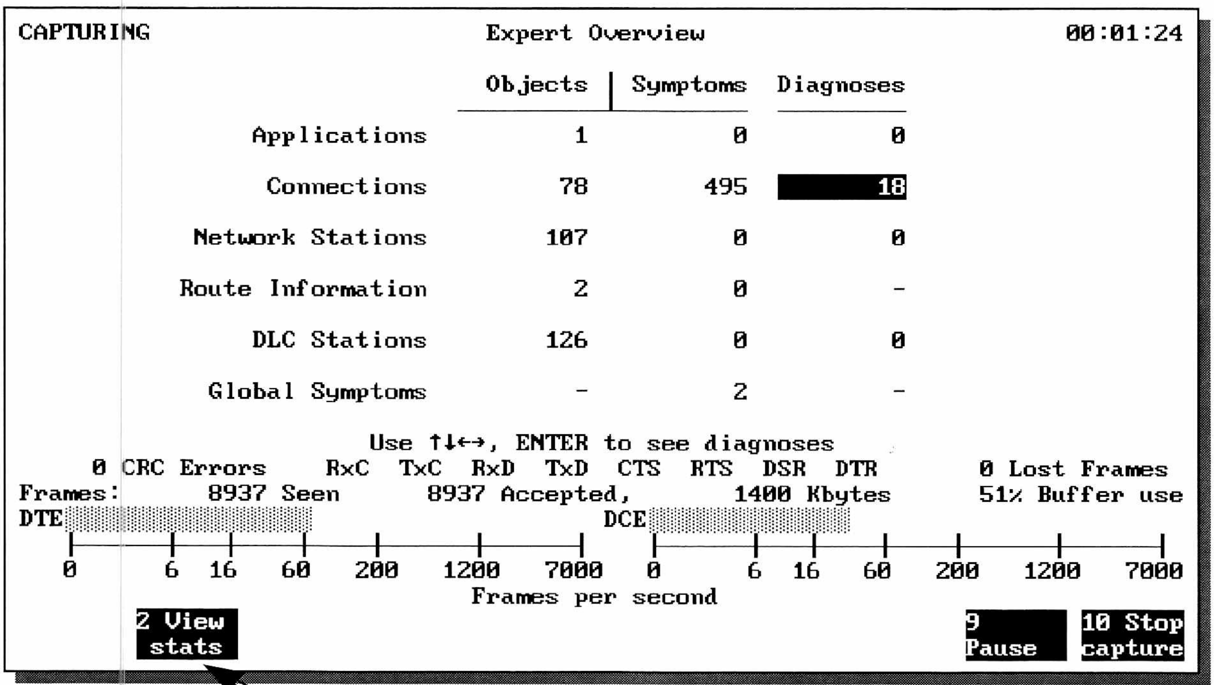
NRZ (Non-Return to Zero) signaling, normally used in computers, means the voltage does not return to zero between adjacent one bits.

NRZI (Non-Return to Zero Inverted) means the ones are zeros and the zeros ones.

Invert means all bits are reversed in value, from ‘0’ to ‘1’ and ‘1’ to ‘0’.

Modulo 8 and **Modulo 128** refer to the data link window size.

Expert Overview Screen



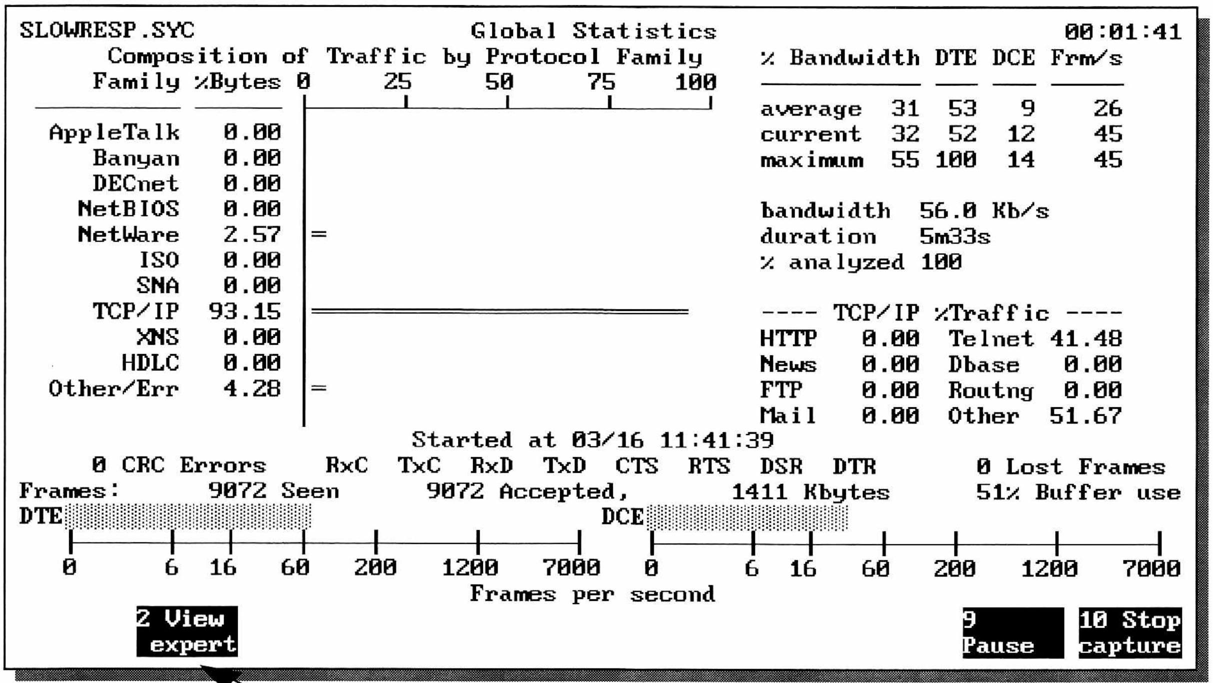
F2 toggles between Expert Overview and Global Statistics.

Demonstration file:
C:\SYCAP\TC107\WELFWAN2.SYC
Press Shift <F10> for continuous capture.

Your screen may look different than this screen. Counters on the left show the number of frames per second from the DTE. Counters on the right show the number of frames per second from the DCE.

A one-line summary shows the status of the line, using the RS-232 indicators. RxC (Receive Clock), TxC (Transmit Clock), RxD (Receive Data), TxD (Transmit Data), RTS (Request to Send), DSR (Data Set Ready), and DTR (Data Terminal Ready). The condition of each lead is shown with an up arrow for a logical one, a down arrow for a logical zero, and a ↕ indicating the lead has changed states in the last second.

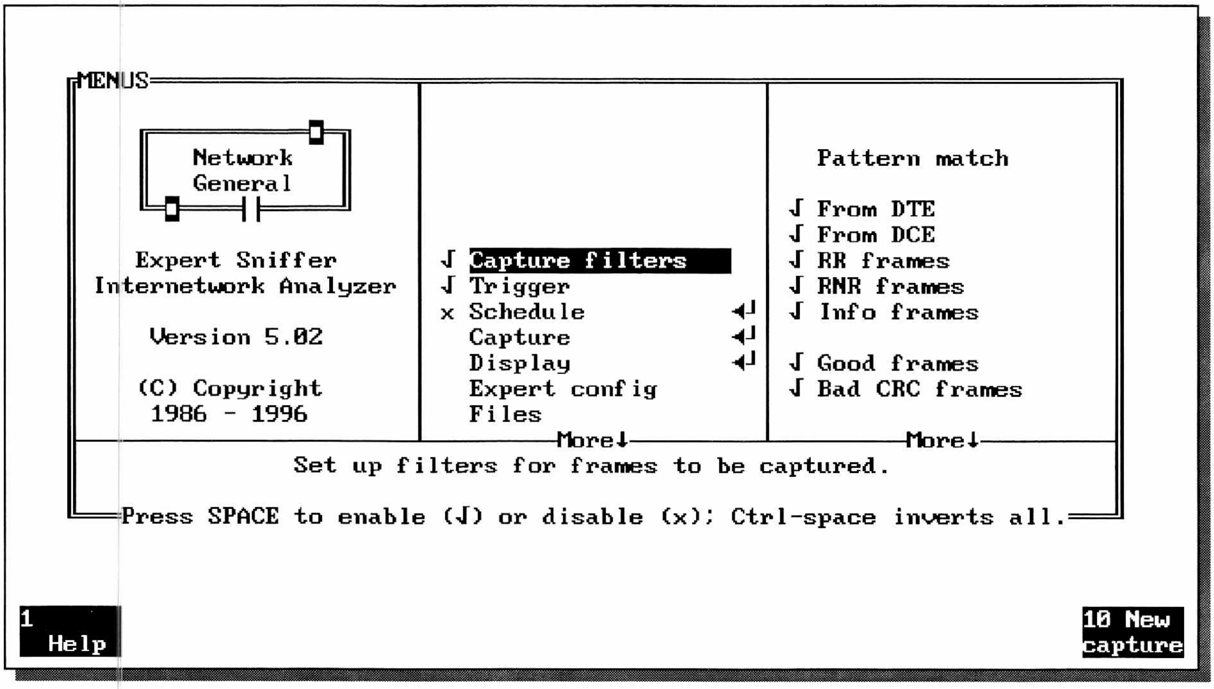
Global Statistics



F2 toggles between Expert Overview and Global Statistics

- **Composition of Traffic by Protocol Family**
  - Frames are categorized according to the highest protocol layer analyzed.
  - Numeric and graphical representation of network traffic percentage in bytes.
- **Bandwidth Utilization**
  - Average, current, and maximum number of frames/second and percentage of bandwidth utilized for both the DTE and DCE. Current bandwidth usage is measured over a one second interval, with measurements taken every 10th of a second, for example 1.0 to 2.0 secs., 1.1 to 2.1 secs. etc. Maximum bandwidth utilization is an average of the maximum high water mark seen from both the DTE and DCE.
- **TCP/IP % Traffic**
  - New for Rev 5.0
- **Run Information**
  - Bandwidth available - theoretical maximum, example 56Kbps, 1.544 Mbps, 19.2Kbps.
  - Duration of capture time between first and last frames in buffer.
  - Start run - time analyzer started capturing traffic.
  - % Analyzed below 100% indicates potential backlog of frames waiting to be analyzed due to heavy traffic loads. When capture stops, the backlogged frames will be analyzed at display time.

Capture Filters



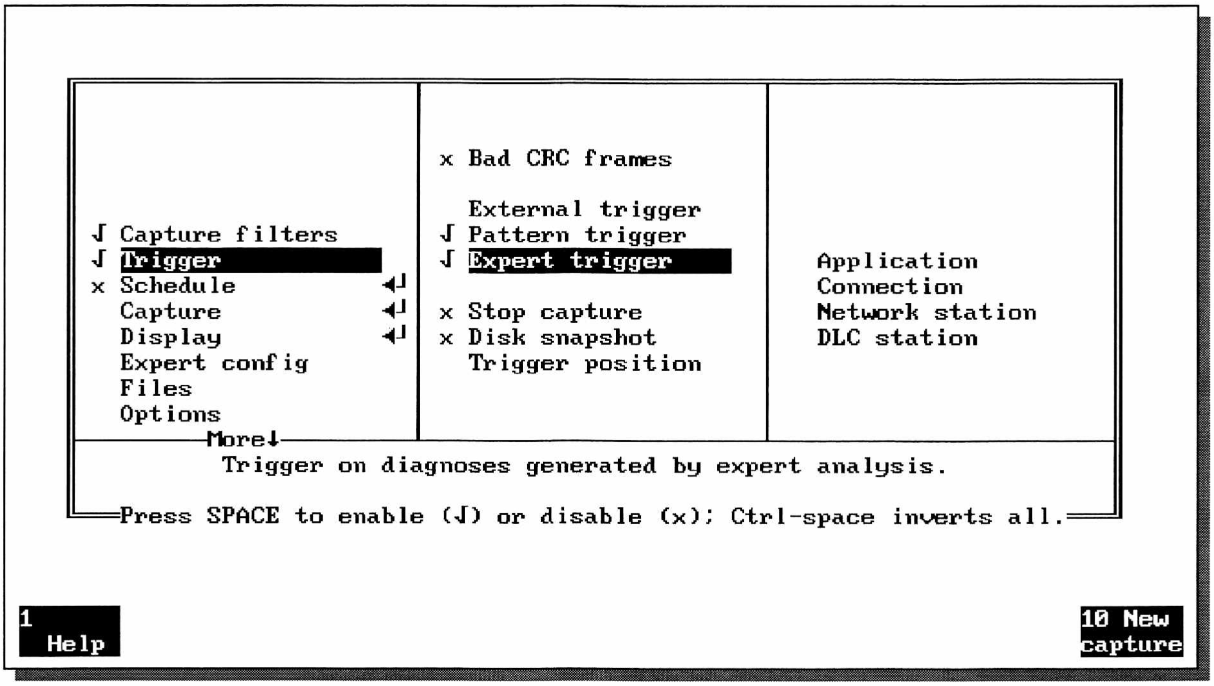
SNIFFER® UNIVERSITY

SIA Overview 4 - 10

Internetwork Analysis and Troubleshooting, 10/96 Rev. 5.0

From DTE	Frames from the bridge/router
From DCE	Frames from the network
RR frames	(HDLC) Receiver Ready - OK to send data
RNR frames	(HDLC) Receiver Not Ready - stop sending data
Info frames	(HDLC) Frames carrying upper layer data

Expert Trigger

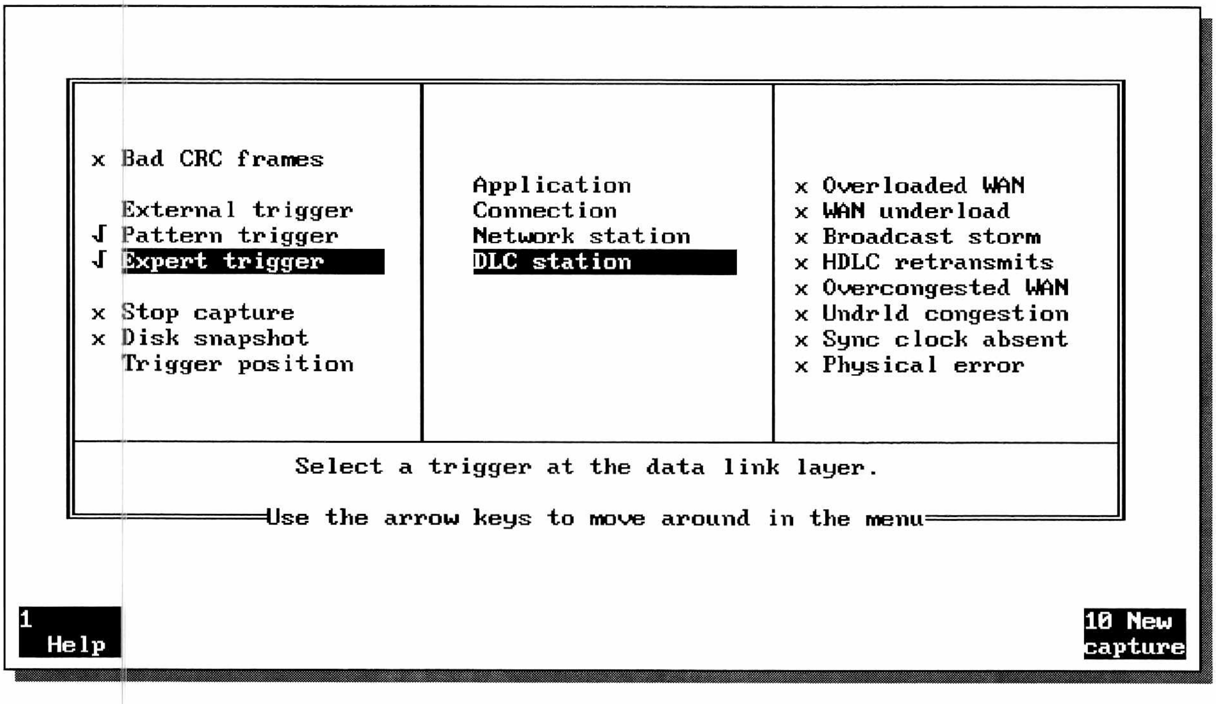


SNIFFER® UNIVERSITY

SIA Overview 4 - 11

Internetwork Analysis and Troubleshooting, 10/96 Rev. 5.0

DLC Triggers



SNIFFER® UNIVERSITY

SIA Overview 4 - 12

Internetwork Analysis and Troubleshooting, 10/96 Rev. 5.0

Network General

The triggers at the **Application**, **Connection**, and **Network station** are the same as the Sniffer Network Analyzer. The **DLC station** triggers, specific to the WAN data link, are based on **Expert settings, Thresholds, DLC station.** In order to understand the DLC station triggers, we must first examine the Expert settings.

Expert Settings

```
  Subnet masks       ◄┘
  Trustee names      ◄┘                                  WAN overload  =  80◄┘
  Frame relay CIRs   ◄┘   Application                    Overload tim  =  60◄┘
                          Connection                     WAN undrload  =  10◄┘
  Expert enables          Network station                Undrload tim  =   5◄┘
  Thresholds              DLC station                    Broadcast sy  =  40◄┘
                                                         Broadcast dg  = 120◄┘
√ Recycle objects                                        ZIP storm     =  10◄┘
                                                         Congestion %  =  10◄┘
                                                         Physical err  =   4◄┘

                       Set thresholds at the DLC station layer.
                 Use the arrow keys to move around in the menu

1                3 Data                                            10 New
  Help           display                                           capture
```

DLC Station Layer Thresholds

- **WAN Overload:** The network load between the DTE and DCE load exceeds the default value of 80% of the potential network bandwidth. Works in tandem with the **Overload tim** to generate a **WAN Overload** symptom (in the Global Symptoms view) and the **Overloaded Network** diagnosis in the DLC stations diagnosis view.
- **Overload tim [er]:** Specifies the duration (in consecutive seconds) of a WAN Overload condition at which the analyzer generates a WAN Overload symptom and an Overloaded Network diagnosis. Possible values range from 1 to 999 seconds; default is 60 seconds.

Demo on how to set thresholds. These may need to be changed to accurately monitor your specific environment.

DLC Station Layer Thresholds

Continued

- **WAN Underload:** The network load between the DTE and DCE load falls below the default value of 10% of the potential network bandwidth. Works in tandemwith the **Underload tim** threshold to generate an **Underloaded Network** diagnosis in the DLC stations layer diagnosis view. Also generates a **WAN Underload** symptom in the Global Symptoms view.
- **Underload tim [er]:** Specifies the duration (in consecutive minutes) of a WAN Underload condition at which the analyzer generates a WAN Underload symptom and an Underloaded Network diagnosis. Possible values range from 1 to 999 minutes; default is 5 minutes.
- **Congestion %:** The point at which the analyzer generates congestion-related thresholds. Calculated differently depending on the type of access protocol used (Frame Relay or HDLC).

The **Congestion %** for HDLC is calculated as a ratio of RNR to RR+RNR frames per minute. For Frame Relay it is the ratio of FECN/BECN frames to total frames.

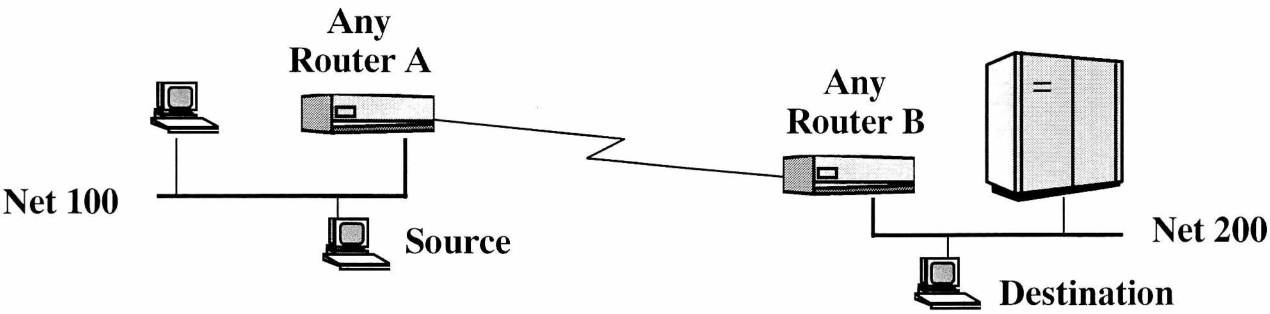
DLC Station Layer Thresholds

Continued

- **Frame Relay symptoms**
  - **Excessive Forward Congestion:** The analyzer generates this symptom when the percentage of Forward Explicit Congestion Notification (FECN) frames to total frames on the link exceeds the **Congestion Percentage** threshold.
  - **Excessive Backward Congestion:** The analyzer generates this symptom when the percentage of Backward Explicit Congestion Notification (BECN) frames to total frames exceeds the **Congestion %** threshold.
- **HDLC symptoms**
  - The analyzer generates the **Overcongested WAN** symptom when the percentage of Receiver Not Ready (RNR) frames to RNR+Receiver Ready (RR) frames exceeds the **Congestion Percentage** threshold.

Excessive Forward and Backward Congestion, HDLC RRs and RNRs will be discussed in more detail in subsequent sections.

Decoding Proprietary Versions of HDLC

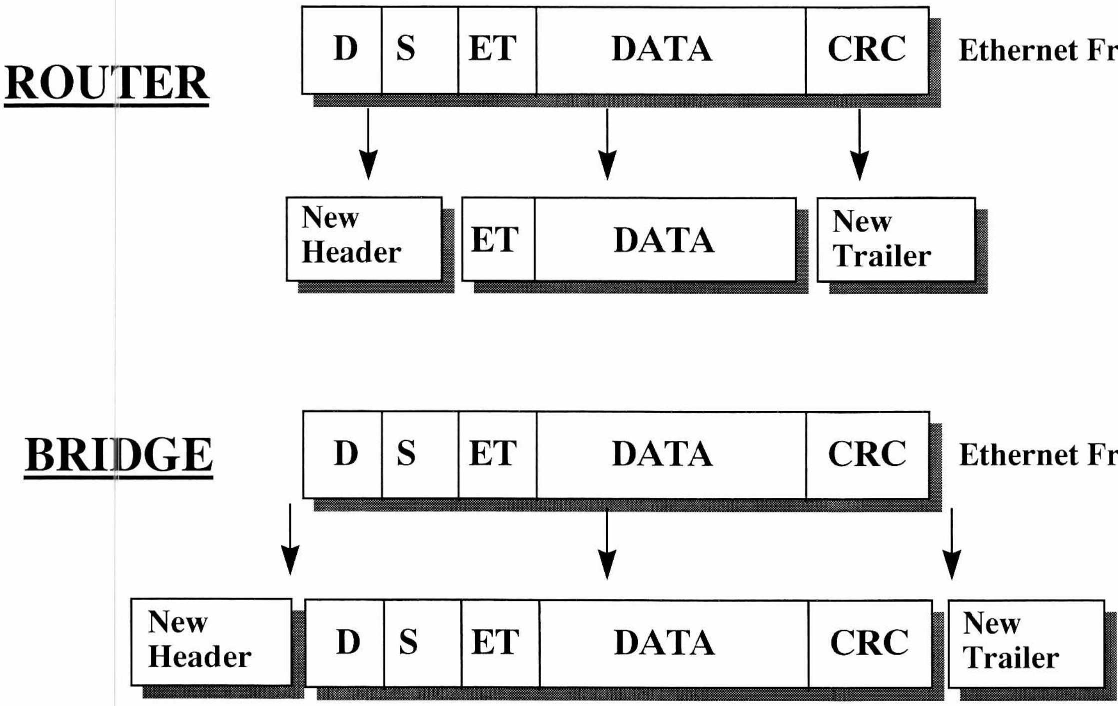


Most bridge/router vendors encapsulate frames in a proprietary header derived from, but not compatible with, HDLC. Since the headers are non-standard, only a bridge/router from the same vendor understands the frame.

When a frame destined for Net 200 reaches Any Router A, A strips off the Ethernet header, adds its proprietary header and sends the frame to Any Router B. When B receives the frame, it strips off the Any Router A header, and encapsulates the data into an Ethernet frame to deliver to the destination.

Standard encapsulation protocols exist like the Point-to-Point protocol (PPP) which theoretically would allow different vendor's routers to communicate, but are not widely implemented at this time. We will cover PPP in a later section.

Encapsulation



SNIFFER® UNIVERSITY

SIA Overview 4 - 18

Internetwork Analysis and Troubleshooting, 10/96 Rev. 5.0

Network General

- To pass a LAN datagram over a WAN link, it must be embedded or *encapsulated* within a WAN frame type.
- The Sniffer Internetwork Analyzer supports SDLC/SNA, HDLC/X.25, Frame Relay, and proprietary Router/Bridge encapsulation.
- Remember a router changes the DLC addresses in a frame before forwarding and a bridge does not.

Protocol Forcing

Protocol Forcing establishes rules for the Sniffer analyzer to decode a protocol it knows how to decode but can not, because:

- The protocol is encapsulated in another protocol (for example for tunneling or encapsulating bridges).
- The protocol is non-standard.
- The frames are illegal or damaged.
- The protocol cannot be recognized by the SIA unless the session establishment sequence is captured.

Note: The LAN Sniffer Analyzer also has Protocol Forcing capability.

Protocol Forcing Procedure

1. Choose a protocol to force from.
   - This is a protocol the SIA can decode without any forcing.
2. Specify rules.
   - Specify any rules or conditions for applying the protocol force.
3. Choose a protocol to force to.
   - This is a protocol that the SIA can decode once the rules are applied.

Hints for Protocol Forcing

- Know what data link layer protocol is being used on the WAN link. Most bridge/routers use their own version of HDLC. Others may use Frame Relay or PPP (Point-to-Point Protocol).
- Have some familiarity with the embedded upper-layer protocols. Some examples:
  - If IP were the embedded layer 3 protocol, the IP header begins with 45.
  - If NetWare's IPX (XNS) were embedded, the IPX header begins with FF FF.
  - If NetBIOS is embedded, look for a 16 byte NetBIOS name in the ASCII data.
  - If SNA is embedded, change the Hex display to EBCDIC, and look to see if the frame data is decoded.


```
DETAIL
HDLC: Address = 05
HDLC: Control field = 00
HDLC:     000. .... = N(R) = 0
HDLC:     ...0 .... = Poll/Final bit
HDLC:     .... 000. = N(S) = 0
HDLC:     .... ...0 = I (Information transfer)
HDLC:
HDLC: [38 bytes: I field]
HDLC:
                    Frame 35 of 1554
HEX                                                          ASCII
0000  05 00 FF FF 00 25 01 11  00 C0 FF EE 00 00 00 00   ..ΔΔ.%...@Δn....
0010  00 01 64 51 00 00 03 00  00 00 C0 2B 5E 4A 40 03   ...Q......@+^J@.
0020  11 11 00 FF 00 FF 00 00                             ...Δ.Δ..
```

In the IPX protocol, FF FF is in the checksum field, although FF FF means the checksum is disabled.

Hints for Protocol Forcing

Continued

- Sometimes it is easier to protocol force using a pattern match based on the first byte or two after the DLC header.
- Look for Ethertypes and LLC SAPs in the frame data as an indication of the upper layer protocol.
- Look for the presence of 6 byte DLC addressing to indicate where the Ethernet or Token Ring frame begins. The broadcast address FF FF FF FF FF FF is an easy one to spot.
- If necessary, you can tell the analyzer to skip bytes of protocols you can't recognize to ones that you can.

Ethertypes and SAPs

Etype	Value	SAP	Value
NetWare	8137	SNAP	AA
XNS	0600, 0807, 0060	BPDU	42
IP	0800	NetBIOS	F0
ARP	0806, 8035	SNA	04, 05, 08, 0C
SNMP	814C	NetWare	10, E0
DRP	6003	XNS	80
LAT	6004	IP	06
LAVC	6007	X.25	7E
IP (VINES)	0BAD, 80C4	ISO	20, 34, EC,
ARP (Atalk)	80F3		FE, 14, 54
AppleTalk	809B		

Note: This is not a comprehensive listing of Ethertypes or SAPs.

Protocol Forcing Exercise

Objective: Perform Protocol Forcing to decode encapsulated protocols.

Background: NetWare (IPX), AppleTalk, and IP packets are being encapsulated within Frame Relay frames. The Sniffer has captured from the Frame Relay link.

1. From the **Main Menu,** select **Options, Frame type, Frame Relay**. Load the file C:\SYCAP\TC107\FSFR01.SYC. Press **F3**, then press **F2** to **View stats**. What are the protocols listed and their percentages? What percentage of the trace is in the **Other/Err** category? What is the bandwidth of this link?

2. Highlight **frame 1**. Turn off the **Summary** window, and turn on the **Detail** and **Hex** windows. Tab into the **Detail** window and highlight the line: **ETYPE: Ethertype = 0800 (IP)**. Note in the Hex display that the highlighted Ethertype [08 00] occurs two bytes into the frame, directly after the Frame Relay header.

3. Go to **frame 30** and perform the same procedure as in step two. What upper-layer protocol is encapsulated in this Frame Relay frame? Is this a bridge, or router encapsulation? Why?

Protocol Forcing Exercise

Continued

4. Look at **frames 2** and **15**. Note that the Null Checksum value **FFFF** is found 16 bytes (**offset 0010**) into both frames. What protocol is indicated by the Null Checksum value **FFFF**? Does this look like a bridge, or router encapsulation? Why?

5. Look at **frames 37** and **60**. Note that the **AppleTalk Ethertype [80 9B]** is found 14 bytes (**offset 0E**) into frame 37, and that the **IP Ethertype [08 00]** is found 14 bytes (**offset 0E**) into frame 60. In both cases, this allows for 2 bytes of Frame Relay header, and 6 bytes each of Ethernet source and destination addressing. Does this look like a bridge, or router encapsulation? Why?

Protocol Forcing Exercise

Continued

6. Using the information obtained by examining the previous six frames, build the following protocol forcing rule:

   Press **F6** for **Display options**, select **Protocol forcing**, **Rule 1**. Change **IF <never> to IF < Frame Relay**>, select **Pattern match** and type "**8137**" for the top **Pattern = XXXX**... field. Then type in **00E** for the offset. Select **OR** as the operation between Patterns. Then type "**0060**" for the bottom **Pattern = XXXX**... field, and type in **00E** for the offset. Arrow back to the left and down to **Skip 000 bytes** and enter **00E**. Move down to **Then <none>** and select **NetWare**. What you have done is told the SIA to decode the data as NetWare when it sees the patterns 8137 or 0060 occurring 14 bytes (00E hex) into the frame.

Protocol Forcing Exercise

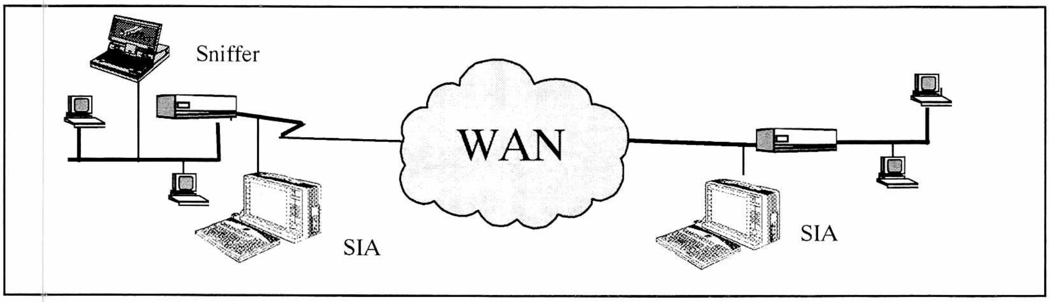
Continued

7 **Rule 2: IF < Frame Relay>**, select **Pattern match** and type "**809B**" for the top **Pattern = XXXX**... field. Then type in **00E** for the offset. Select **OR** as the operation between Patterns. Then type "**0800**" for the bottom **Pattern = XXXX**... field, and type in **00E** for the offset. Arrow back to the left and down to **Then <none>** and select **Ethernet**. This tells the SIA to decode the frame as Ethernet when it sees the patterns 809B or 0800 occurring 14 bytes (00E hex) into the frame.

8 Press **F3** to redisplay the data. Tab into the **Summary** display, and verify that the frames are now decoded. Press **F3** to display **Global Statistics**. What are the protocols listed and their percentages?

9. Press **F5** to go to main menu. Select **Files, Save, Setups, Enter** and save setup as **FSFR01**.

Troubleshooting with the SIA



- If possible, set up a Sniffer LAN Analyzer on the local LAN segment of the Router and the SIA on the local WAN segment of the Router. Using both will allow you to look for problems with router configuration and protocol translation, in addition to troubleshooting the respective LAN and WAN.
- Once the integrity of the local LAN/WAN internetwork has been verified, begin troubleshooting end-to-end across the WAN, using two SIA's or the Distributed Sniffer System.

Troubleshooting with the SIA

Continued

- Take a "layered" approach to troubleshooting. For example, begin with the Physical layer and move up through the OSI model. Prove each layer is healthy before moving up. Global failures typically are found at the lower three layers.
- Examine the Global Statistics and Expert Overview screens. Look for Expert diagnosis such as a **High rate of physical errors by DTE, WAN Overload, Overcongested WAN** at the **DLC stations** layer and **Global Symptoms**, which could affect the wide area link.
  - If the **WAN Overload** (80% utilization for 60 seconds) diagnosis frequently encountered, consider purchasing additional bandwidth.
  - If the WAN is not overloaded nor congested, **purchasing a higher speed line will not correct the problem!**

Troubleshooting with the SIA

Continued

- To better tune your WAN, minimize unnecessary broadcast traffic going over the wide area.
  - Check the frequency of your management stations polling over the wide area and adjust accordingly.
  - Investigate filtering options on your routers and bridges to eliminate unnecessary outbound and inbound broadcast traffic. In packet switched networks which may charge by the packet, reducing unnecessary traffic becomes even more important.
- If the WAN link tests fine, examine potential network layer routing problems such as missing RIP packets, SAP floods, corrupted routing tables, congested routers dropping frames, modulo.

Summary

- There are features unique to the Sniffer Internetwork Analyzer (SIA).
- Adjust the Expert thresholds after you have carefully analyzed your network to more accurately reflect it's characteristics.
- Use protocol forcing to enable the SIA to decode encapsulated protocols.
- Information provided by the SIA quickly helps you identify, troubleshoot and optimize WAN area connections.

T-1 Networking

Objectives

On completion of this section you will:

- Know the components of a T1 connection, the interface and how voice is carried on the line.
- Understand Bipolar and Bipolar with 8 Zero Substitution (B8ZS) signaling and how the clock is embedded into the signal.
- Be able to differentiate the 2 frame formats and the 4 T1 channel types.

This section specifically references T-1 connectivity. Another alternative to T1 is E1 which is used outside of North America. The major difference in the two is that T1 is made up of 24 DS0's and E1 is made up of 32 DS0's. We will cover DS0's in the upcoming material.

Overview of T-1

- T1 allows integration of voice, data, facsimile, and image into high-speed backbone networks.
- The T-1 land line is a run of twisted copper pairs with digital repeaters inserted one mile apart. Due to distortion and jitter, no more than 50 repeaters may be connected in series.
- Long-haul distances usually employ microwave relay facilities and provides medium for about 75% of US long distance voice traffic.*
- T1 is the primary digital full-duplex transmission system in North America for digitized voice and data.

The term T-1 (T for Time Division Multiplexing) originated with the phone company to interconnect central offices (COs), and referred to a very specific type of equipment and cabling. In common usage, it generically refers to a transmission rate of 1.544 Mbps.

Introduced in the 1960s as a way for COs to connect 24 voice grade digital lines, it was not widely tariffed and available for public use until 1983.

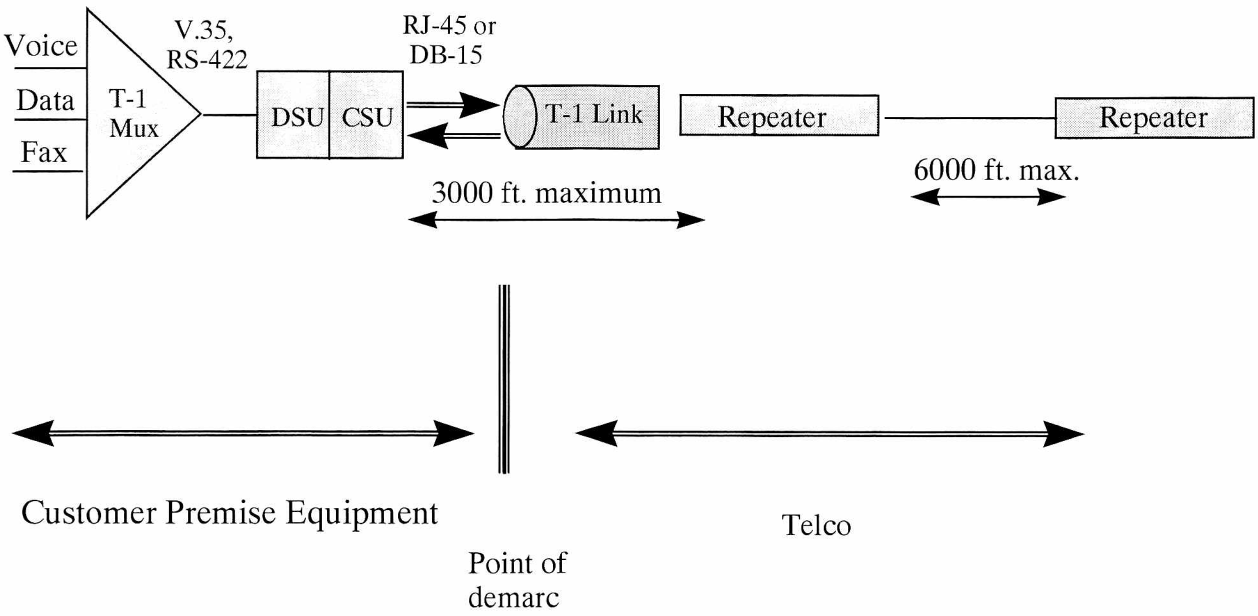
The one mile marker is the distance between manholes in large cities.

* The typical transit time for a T-1 circuit across the US is 40-50 ms. It can be as little as 10 ms for a hundred mile leg. (Voice circuits have a higher delay.)

Customer Premise Equipment

- **Customer premise equipment** (CPE) is owned by and located at the customer's location. CPE includes: multiplexers, CSUs/DSUs, PBXs, T-1 channel banks, computers, front end processors, and other DTEs.
- **Data terminal equipment** (DTE) provides the source of the transmitted signal and the destination of the received signal.
- **Point of demarcation (demarc)** is the physical point of separation between responsibilities of the user (customer) and responsibilities of the telephone company (telco).

The Big Picture



AT&T specifies 3000 feet maximum from the last repeater to the CSU. All other repeaters have a 6000 foot maximum. This is to ensure adequate signal amplitude at the Network Interface which is the termination of the T-1 span at the customer premises.

T-1 Interface

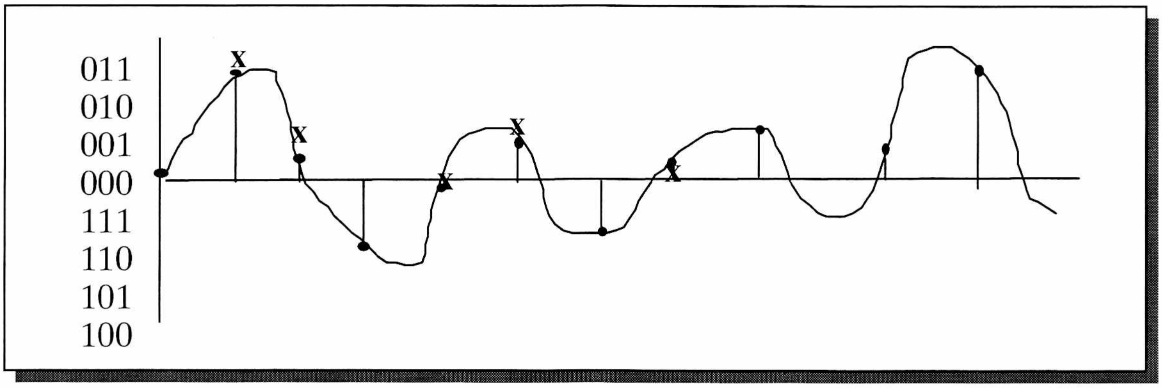
A dedicated T-1 will appear at the customer's end as two wire pairs: one for transmit and one for receive.

DB-15 PIN				RJ-48C PIN	
11	B	Receive	R	1	Pair
3	A	Receive	T	2	
7,8,12,14,15		No connection		3,6	
9	B	Transmit	R1	4	Pair
1	A	Transmit	T1	5	
N.A.		Optional Shield		7,8	
5,6,10,13		Reserved for Telco		N.A	

The physical connector used to be a DB-15 but the current standard is an RJ-48C.

Digitized Voice

- T-1 circuits transmit information in digital form.
- Since voice is analog, a codec is used to translate the analog voice into digitized voice, using a technique known as Pulse Code Modulation (PCM).



SNIFFER® UNIVERSITY

T1 Networking 5 - 7
Internetwork Analysis and Troubleshooting, 10/96 Rev. 5.0

Network General

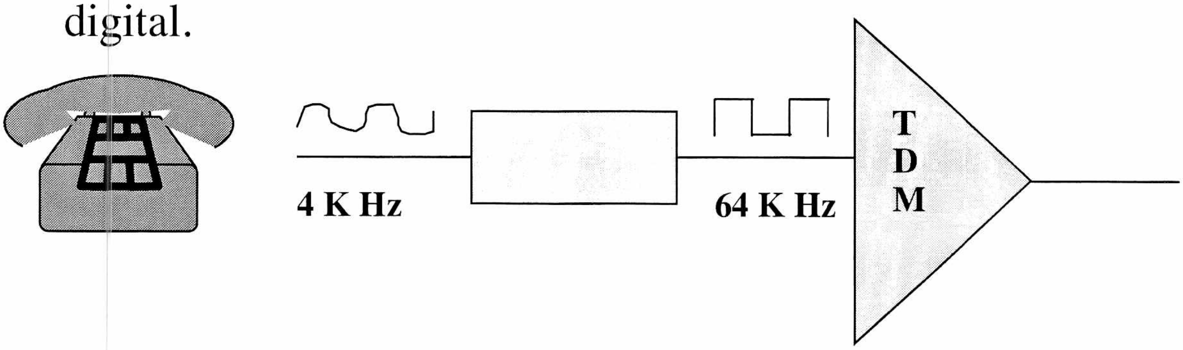
With PCM, the analog signal is sampled 8000 times a second and the amplitude of each sample gets represented with 8 bits. As a result, an analog signal gets converted to a digital bit stream of 64,000 bits.

Why is the signal sampled 8000 times a second? To adequately represent voice in a digital format, you must sample at a rate equal to twice the frequency of voice (4000 Hz).

The signal will be represented by the nearest digital value - the difference between the nearest binary representation of the signal and the actual signal is **quantified noise (X).**

Channel Banks

- Channel Bank is a TDM that consists of a main module and 24 channel cards. Each card determines what type of information gets transmitted over that specific DS0 or channel. 4 Wire E&M cards enable analog voice to be sent out as a digital signal.
- A COder/DECoder or codec converts the analog signal to digital.



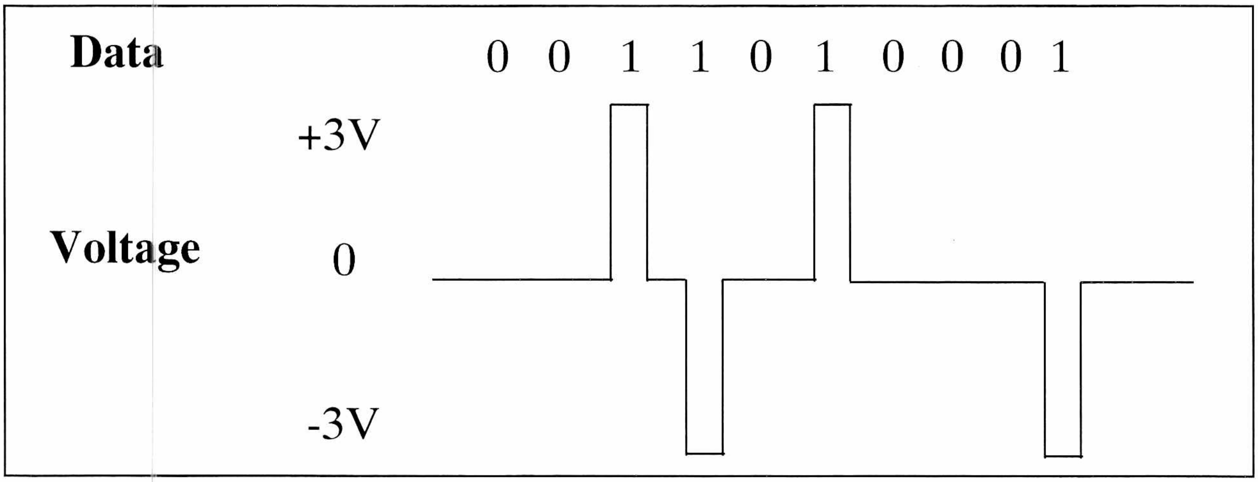
Different channel cards can be used for different signals. You have voice cards that convert the signal to digital 64K. You also have cards that adapt the signal to lower speed circuits, such as 2400, 4800, and even 9600 BPS circuits. The one thing they all have in common is, they are taking up a full 64KBPS worth of bandwidth on your T1. Some channel banks have diagnostic capability.

DSU: Digital Service Unit

- Converts one or more subrate signals (less than the T-1 rate) to a T-1 signal.
- Converts input signal to bipolar.
- Extracts timing from the received signal and provides timing for the transmitted signal.
- Has remote and manual loopback capabilities.

A DSU is like a digital modem.

Bipolar Signaling



T-1 signals use Alternate Mark Inversion (AMI) line Return to Zero (RZ) encoding. Consecutive ones or marks are of opposite polarity. Zeros or spaces are zero volts. Voltage returns to zero after consecutive marks.

Who's Got the Time?

- In T-1 transmissions, there is no separate clocking signal.
- Timing is recovered from the received data.
- Data must contain enough information to derive clock.
- Zeros produce a steady state voltage and no useful timing information. Ones are used to determine timing.
- Clock is recovered by a tuned resonant or phase locked loop circuit.
- Jitter is a condition where the phase of the output pulses is ahead of, or behind the master clock. Jitter can accumulate through repeaters and may be no more than 14 bit times.

SNIFFER® UNIVERSITY

T1 Networking 5 - 11
Internetwork Analysis and Troubleshooting, 10/96 Rev. 5.0

Network General

Switches in the public network do receive a definite clock. T-1 networks that do not run through a switch need to supply a clock near the T-1 frequency.

Ones Density

- To ensure enough ones are transmitted, the specification for T-1 transmission facilities, AT&T Compatibility Bulletin 19, states that:
  - There shall be at least **N ones in every 8(N+1) bits.**
- As a result, no more that 15 consecutive zeros can be transmitted.
- Ways the CSU or mux can accomplish ones density:
  - "Jam bit 7" - place a 1 in the 7th bit of an all-zero byte.
  - Bit stuffing - substitute a one for a zero as required to ensure sufficient ones density.. This may cause problems with the applications.
  - Invert data so all zeros are ones and ones are zeros (if the data has a lot of zeros).

SNIFFER® UNIVERSITY

T1 Networking 5 - 12

Internetwork Analysis and Troubleshooting, 10/96 Rev. 5.0

Network General

Older T-1 repeaters would tend to oscillate if they lost synchronization. When they oscillated, that signal would couple to adjacent wires and interfere with other T-1 lines. This problem was very difficult to isolate.

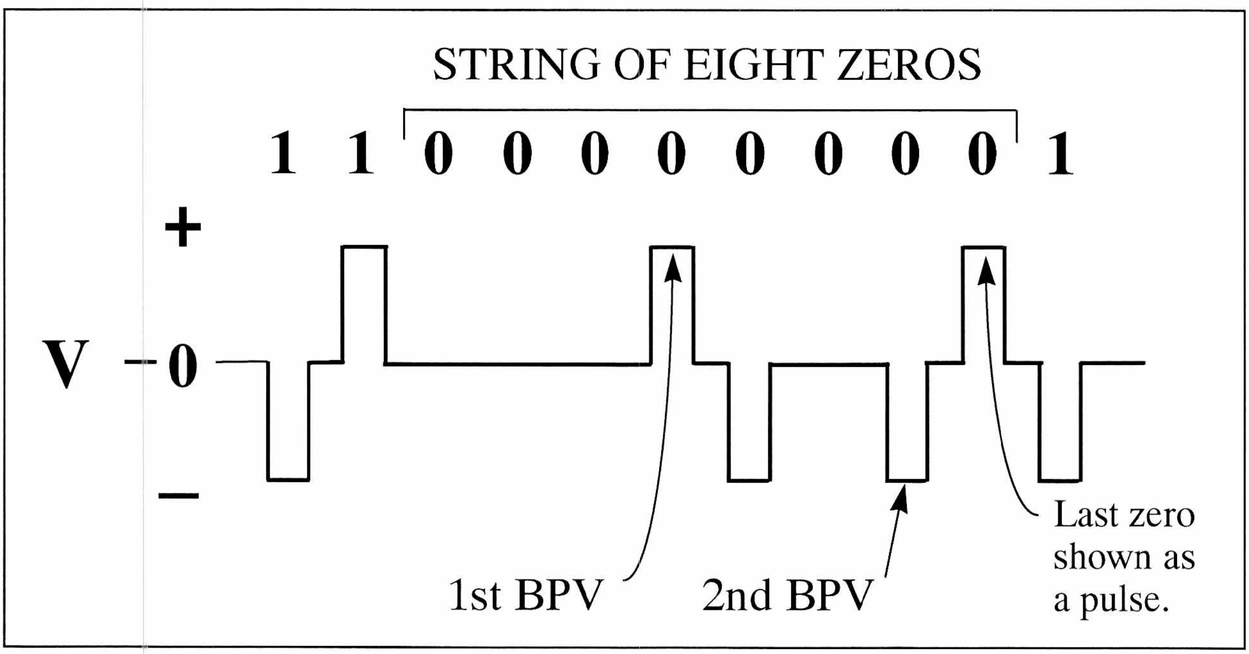
Newer repeaters are not as prone to oscillate and the FCC has relaxed the ones density rule to up to 80 zeros in a row. The average density must still be 12.5 %.

We will talk about how bit-stuffing is accomplished in a later section.

Bipolar with 8 Zero Substitution (B8ZS)

- Because of the possibility of long strings of zeros occurring in data (vs. voice) transmissions, data circuits need a method to ensure one's density without data corruption.
- B8ZS replaces any string of eight consecutive zeros with two intentional bipolar violations (BPVs). This results in network timing being maintained.
- Both ends of the T-1 circuit must use B8ZS. Intervening network equipment must not correct BPVs.

B8ZS
Continued



The Single Frame

- The frame in a channel bank represents a sample of each of 24 channels.
- Each value is represented by an 8 bit word.
- The 8 bit word occupies a **time slot** which is 8 bit times.
- With a sampling rate of 8,000 times a second, one time slot represents 64,000 bits.

The digital signal level zero or DS-0 is 64,000 bits per second.

The sampling rate of 8K times a second comes from the Nyquist theorem which shows that analog data reconstructed from digital, will contain all the original vocal quality, if the sampling rate is at least two times the highest voice frequency.

Two Frame Formats

Superframe (also referred to as D4 format)

The data in one frame is 192 bits and one framing bit.

24 time slots x 8 bits per time slot	8000 x a second sampling rate x 192 bits per frame	+	8000 framing b/s
192 bit frame	1,536,000 bps		**1.544 Mbps or DS-1**

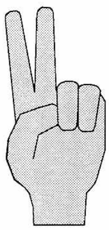
> A super frame consists of 12 - 193 bit frames (2316 bits total).
>
> Framing bits are used for synchronization and occur in a fixed pattern of 1s and 0s: **100011011100.**

To find the 193rd bit (the framing bit), the receiver looks for a predefined pattern that repeats every 12 frames: 100011011100.

The commercial chipsets currently used, can find framing patterns in milliseconds. These circuits can sync up two channel banks so quickly that a loss of sync is barely audible on a voice call.

An Out Of Frame (OOF) error is generated on the T1 pod when any 2 out of 5 framing bits are in error.

Two Frame Formats



Extended Super Frame - The ESF was designed to eliminate much of the overhead associated with D-4 framing and allow live monitoring. With ESF, the D4 superframe is extended from 12 to 24 frames (4632 bits). The 8 kbps of overhead is divided into three separate channels:

- A 2 kbps channel for framing
- A 2 kbps channel for CRC-6
- A 4 kbps channel, called the Facility Data Link (FDL), for diagnostic control and transmission of performance statistics

Improvements in synchronization circuits reduced the need for framing synchronization to less than 8 kbps.

CRC-6 is a six-byte cyclic redundancy check for each ESF which is calculated by the transmitter and verified by the receiver to detect bit errors.

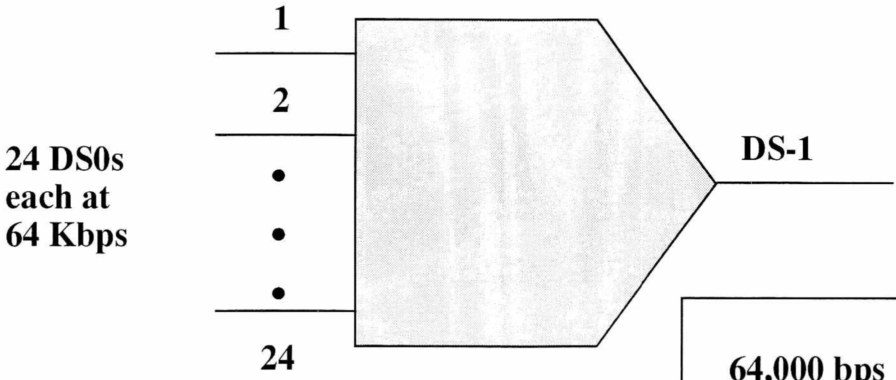
Some management systems utilize the FDL bit for diagnostics (for Ex. CSU’s). If the local loop is a fractional or not a full T1, then the FDL bit is lost and anything attempting to take advantage of the FDL bit, does not work.

CSU: Channel Service Unit

- A CSU is used to protect the Carrier from external interference transmitted from the customer's DTE.
- The CSU regenerates the transmit and received signals.
- CSU's support both local and remote loopback capability which can help isolate the source of a problem.
- The CSU provides a "keep alive" signal to the network when the attached equipment fails or is disconnected.
- It performs ones density enforcement.
- CSUs can be used to calculate and collect Extended Super Frame error statistics.

When the T-1 mux fails or is disconnected from the network, or for whatever reason the CSU no longer sees a signal from the DTE, it will send continuous 1's, or an "All 1's" signal onto the network. The carrier sees this as a RED alarm.

The Digital Building Block



64,000 bps	Channel rate
x 24	# Channels
1,536,000	
+ 8000 bps	Control
1.544 bps	T-1 Speed

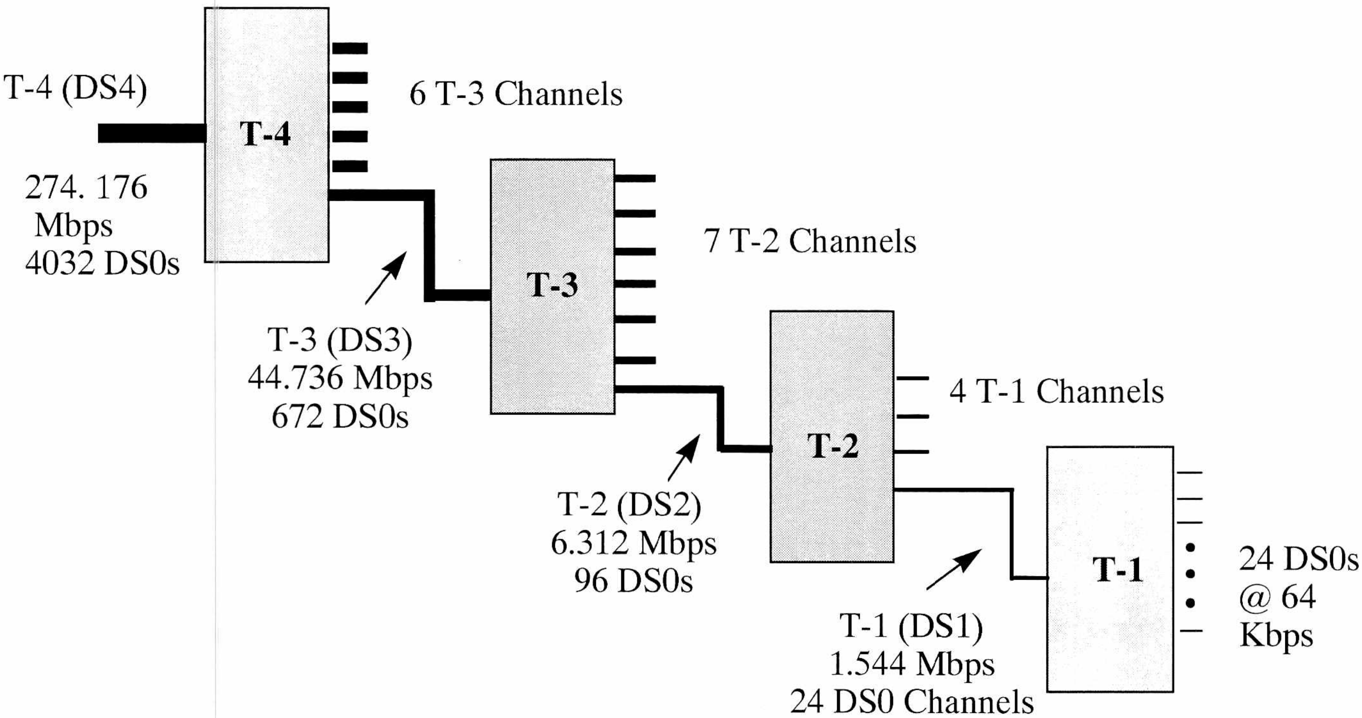
A single digitized voice signal takes 64,000 bps. This is known as a digital signal level zero, or DS-0.

In North America, Japan, and Australia, the T-1 standard of 1.544 Mbps is used.

In European and other CCITT countries, 30 voice/data channels are mutiplexed with two control channels for an aggregate speed of 2.048 Mpbs (E-1 standard).

Both of these composite speeds are referred to as DS-1.

The Digital Hierarchy



SNIFFER® UNIVERSITY

T1 Networking 5 - 20

Internetwork Analysis and Troubleshooting, 10/96 Rev. 5.0

Network General

A typical application would be to connect remote sites to a central site via a 56/64 Kbps leased line. Connecting major sites together may require T-1 transmission speeds, to accommodate the voice and data traffic. To transport video will require at least T-3 transmission facilities. This signal is known as a DS-3.

Four T-1 Types

Normal - Uses all 24 channels separately at 64 Kbps or 56 Kbps each.

Subrate - Takes a 64 Kbps channel and breaks it into many 2.4 Kbps, 4.8 Kbps, 9.6 Kbps, etc.

Fractional - Adds DS0s channels together for higher data rates.

2 Channels = 128 Kbps
4 Channels = 256 Kbps
8 Channels = 512 Kbps **...**

Full bandwidth - Uses the entire T-1 bandwidth as one channel at 1.544 Mbps.

SNIFFER® UNIVERSITY

T1 Networking 5 - 21
Internetwork Analysis and Troubleshooting, 10/96 Rev. 5.0

Network General

T-1 Errors Exercise

Objective: To examine a T-1 link for proper communication and operation.

Background: Remote X-Windows and Telnet users are reporting that periodically their sessions hang. An SIA has been attached first at one end of a routed T-1 link, and then later at the other end.

1. **Load** the trace file C:\SYCAP\TC107\TLNT-01.SYC and press **F3** to display.
2. Press **F2** to View Statistics. Examine the Bandwidth field in the lower right quarter of the screen: what is the bandwidth of the circuit? Judging from the % Bandwidth Utilization fields in the upper right quarter of the screen, was the network overloaded?
3. Press **F2** for Expert Display. Highlight **Connection Symptoms** and press **Enter**. What symptom is associated for which connection?
4. Press **ESC** to return to **Expert Overview**, highlight **Connection Diagnoses**, and press **Enter**. Given the symptoms of the previous question, what has Sniffer analyzer determined about one of the two nodes?

T-1 Errors Exercise

Continued

5. Press **F3** for Data Display. Let's name the two nodes presently using the T-1 link: press **F6** for Manage Names, **cursor** across to Edit Names, press **Enter**, and highlight 166.7.140.65. Press **Enter**, give the node the name Client, and press **Enter**. Using the same method, name the other node, 166.7.147.193 as Host. When finished, press **ESC** and then press **F3** to display the data.
6. Press **F6** for Display Options, enable **Two-Station Format**, **Hex** window, and set the **Name Width** to 11. Press **F3** to display the data. Your screen has now been "optimized" for viewing communication between two nodes.
7. Frames 1-3 are TCP's "3-way handshake", frames 4-11 are Telnet negotiation, and if you examine the Hex window of frame 13, you'll see the "login:" prompt from Host to Client.
8. If you follow the communication and character echoing further, you'll see that user "TESTL11" logs in and is prompted for a password in frame 50.

T-1 Errors Exercise

Continued

9. From the non-echoed characters of frames 52-66, what password does the user enter? Based on what we have seen so far, is there anything abnormal about the Telnet session setup and login?

10. The user, TESTL11, goes on to perform the UNIX command "cd /etc" and "more motd.old", after some more character corrections.

11. Frame 144 represents the "banner page" that Host sends to "paint" Client's screen. From the SIA's perspective, what is unusual about the next frame? Does Client send a TCP acknowledgment to Host for frame 144? How much time elapses between frames 144 and 145?

12. Examine the Delta Times between the subsequent frames until the end of the trace file. What do you notice about TCP's retransmission algorithm?

T-1 Errors Exercise

Continued

13. At this point we can deduce that the user's report of a "hung session" is accurate. Using the OSI model as a general reference, briefly list some possible reasons why this may have occurred.

14. Now let's look at a similar session with the ESIA attached to other end of the T-1 link. **Load** and **display** the trace file C:\SYCAP\TC107\TLNT-02.SYC.

15. You may wish to use **Manage Names**, **Edit Names** to name the node 166.7.140.193 as Client2 and 166.7.3.65 as Host2.

16. As in the earlier trace file, we see the "banner page" in frame 10 but this time the Telnet session has already been established.

17. Press **F6** for Display Options, **cursor** across and enable **Flags**. Also enable the **Detail** window.

T-1 Errors Exercise

Continued

18. What is unusual about frame 11? In the Summary window, examine the **Flags** field: which flag has been set? *Hint: look at the beginning of the frame in the Detail window to determine the meaning of the flag.* At which OSI layer does this error occur? List some reasons why this may have occurred. *Note: you may wish to go back and determine if SIA spotted these errors by examining the DLC Stations Symptoms, if any, on the Expert Overview screen.*
19. Examine the Flags and Delta Times of the remaining frames. What can we conclude about the condition of the frames arriving from the network: is the receiving router "at fault"? *Hint: has the receiving router received the frame yet?*
20. Considering the previous trace file, TLNT-01.SYC, is the sending router "at fault"? If not, where might the fault lie for the condition of the frames? In terms of problem resolution, how would you proceed from here?
21. If you're interested, compare the "banner page" of TLNT-02.SYC with that of TLNT-01.SYC and you will see the characters that have changed in transit.

Summary

- T1 lines carry voice, data, FAX or image data from a DTE on high speed lines which are interfaced through CSU/DSU's at the DEMARC on the customer premises.
- Bipolar and Bipolar with 8 Zero Substitution (B8ZS) signaling are used and the clock is embedded into the signal.
- T1 uses either Superframe (D4) or Extended Super Frame formatting.
- There are 4 T1(E1) channel types: Normal, Subrate, Fractional and Full Bandwidth which allow the bandwidth to be split and allocated differently.

HDLC

SNIFFER® UNIVERSITY

HDLC 6 - 1

Network General

Objectives

On completion of this section you will:

- Know the types of HDLC stations and configurations.
- Understand the three modes of operation.
- Be able to recognize the HDLC frame format and how the Detail window decodes the types of frames.
- Know how to associate the LAPB address fields with a particular device.
- Recognize the sequence of frames of a normal setup, data transfer and shutdown of an HDLC session.
- Know how the individual bits in the control field affect and indicate the operation of the connection.

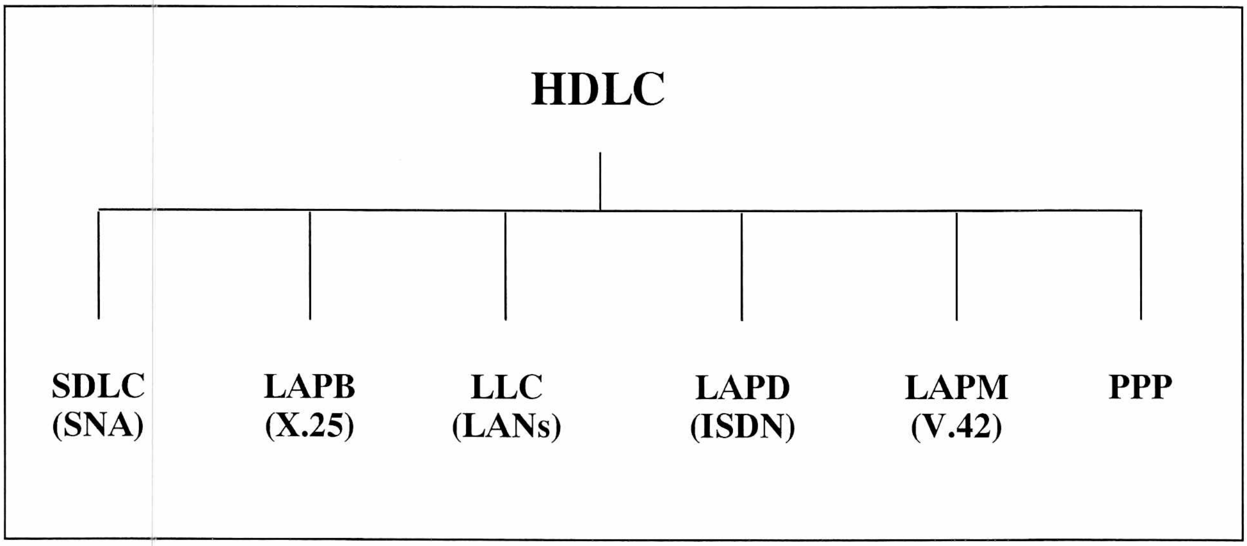
Data Link Layer Review

The services of a data link layer protocol may include:

- Synchronization of data.
- Controlling data flow to prevent the sender from overwhelming the receiver with data.
- Error detection and recovery.
- Determining the identity of communicating stations.
- Distinguishing between data and control signals.

A data link layer protocol only provides service on a point-to-point link. It's up to a higher layer protocol to provide end-to-end services.

High-level Data Link Control: the Mother of all DLC Protocols



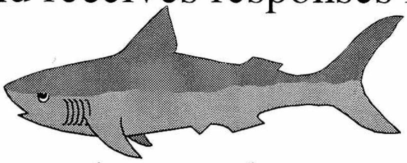
LAPM	Link Access Procedure Modem
LAPB	Link Access Procedure Balanced
LAPD	Link Access Procedure D channel
LLC	Logical Link Control
SDLC	Synchronous Data Link Control
PPP	Point-to-Point Protocol

HDLC supports both half-duplex and full-duplex transmission, point-to-point and multipoint configurations, as well as switched and non-switched lines.

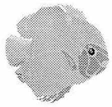
Technically speaking, SDLC, introduced by IBM in 1972, was the first bit-oriented synchronous protocol. ISO later standardized HDLC which is said to encompass all the functionality of SDLC, and is probably best thought of as a superset of SDLC.

Types of HDLC Stations

- A **primary station** is the master of the data link and transmits commands to and receives responses from the secondary stations.



- A **secondary station** is dependent on the master and issues responses when polled by the primary station. LAP uses this relationship.



- The **combined-station** approach (also referred to as peer-to-peer) is used by LAPB. Either the DTE or the network can transmit and receive commands at will and take advantage of the full-duplex channel.

SNIFFER® UNIVERSITY

HDLC 6 - 5

Internetwork Analysis and Troubleshooting, 10/96, Rev. 5.0

Network General

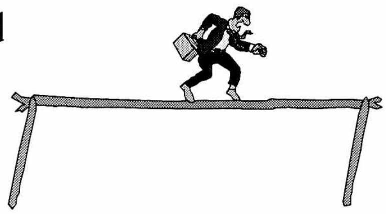
The **primary** station controls the data link. This station acts as a master and transmits command frames to the secondary stations on the channel. In turn, it receives response frames from those stations. If the link is multipoint, the primary station maintains a separate session with each station connected to the link.

The **secondary** station acts as a slave to the primary station. It responds to the commands from the primary station in the form of responses. LAP uses this approach.

In the **combined station** approach the DTE and network can transmit and receive commands and responses to and from each other without waiting for a data solicitation. It makes no sense to wait for permission to send data when a full-duplex path is available in each direction between the DTE and the network. Used by LAPB.

Types of HDLC Configurations

- An **unbalanced** configuration is used in SDLC networks where one primary controls one or more secondaries. The primary is responsible for establishing and maintaining the link.
- The **symmetrical** configuration is not very popular today. This configuration provides for two independent, point-to-point unbalanced stations, with each station having primary and secondary status.
- A **balanced** configuration is used by LAPB and consists of two combined stations. Each station has equal status, equal responsibility for link maintenance, and can send commands to elicit responses. The other side could answer with a command of its own.



SNIFFER® UNIVERSITY HDLC 6 - 6 Internetwork Analysis and Troubleshooting, 10/96, Rev. 5.0 Network General

An **unbalanced** configuration provides for one primary station and one or more secondary stations to operate as point-to-point or multipoint, half duplex or full duplex, switched or nonswitched. The configuration is called unbalanced, because the primary station is responsible for controlling each secondary station and for establishing and maintaining the link. Most SDLC configurations use this approach.

A **balanced** configuration consists of two combined stations connected point-to-point only, half duplex or full duplex, switched or nonswitched. The combined stations have equal status on the channel and may send unsolicited frames to each other. Each station has equal responsibility for link control. Typically, a station uses a command to solicit a response from the other station. The other station can send its own command as well. LAPB uses the balanced option of HDLC, but only on full duplex, point-to-point links.

Data Transfer Modes of Operation

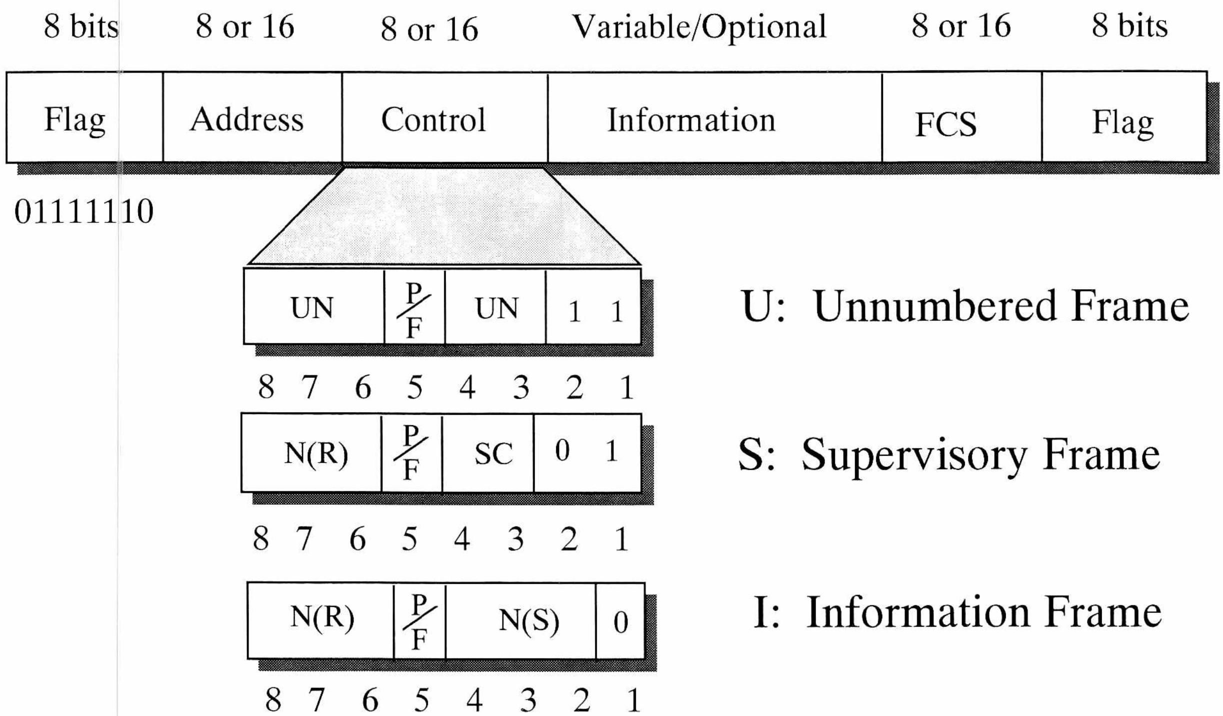
- **Normal response mode (NRM)** - used by SDLC, NRM requires the secondary station to receive explicit permission from the primary in order to transmit.
- **Asynchronous response mode (ARM)** - used by LAP, ARM allows a secondary station to initiate transmission without receiving explicit permission from the primary. A secondary may only transmit when it detects an idle condition when operating in half duplex mode or at any time when in full duplex mode.
- **Asynchronous balanced mode (ABM) -** used by LAPB, LAPD, and LLC Type 2, ABM uses combined stations that may initiate transmissions at any time without receiving permission from the other station.

While the HDLC stations are transferring data, they communicate in one of three modes of operation.

Normal response mode is found on multi-drop lines where the primary controls the link and periodically polls the secondaries. The primary station controls the link by issuing polls to the attached stations (usually terminals, PCs, and cluster controllers).

Asynchronous balanced mode is used over point-to-point links and does not incur the overhead and delay associated with polling.

HDLC Frame Format



SNIFFER® UNIVERSITY

HDLC 6 - 8

Internetwork Analysis and Troubleshooting, 10/96, Rev. 5.0

Network General

Demonstration file: C:\SYCAP\TC107\UNSUPINF.SYC

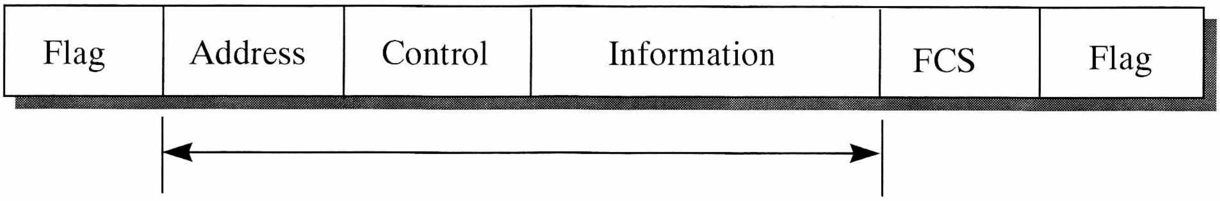
The flag is used for synchronization and signals the beginning and end of the frame.

The 1st and/or 2nd bits of the control byte determine the frame type - U, S, or I.

In LAPB, the transmitter computes a FCS or cyclic redundancy check using modulo 2 division on the Address, Control, and Information fields plus 16 leading zeros.

The FCS (or CRC) field is typically 16 bits for HDLC.

HDLC Capture Range



The Sniffer Internetwork Analyzer doesn't capture the Flags because doing so would fill the capture buffer with non-data.

The Sniffer Internetwork Analyzer does not report the **FCS value** but will report if it's bad.

Flags

- All frames must start and end with the flag field.
- Stations attached to the data link monitor the link for the flag sequence.
- Stations recognize the following bit sequences:
  - 01111110: Flags
  - At least 7, but fewer than fifteen 1s: Abort
  - Fifteen or more 1s: Idle

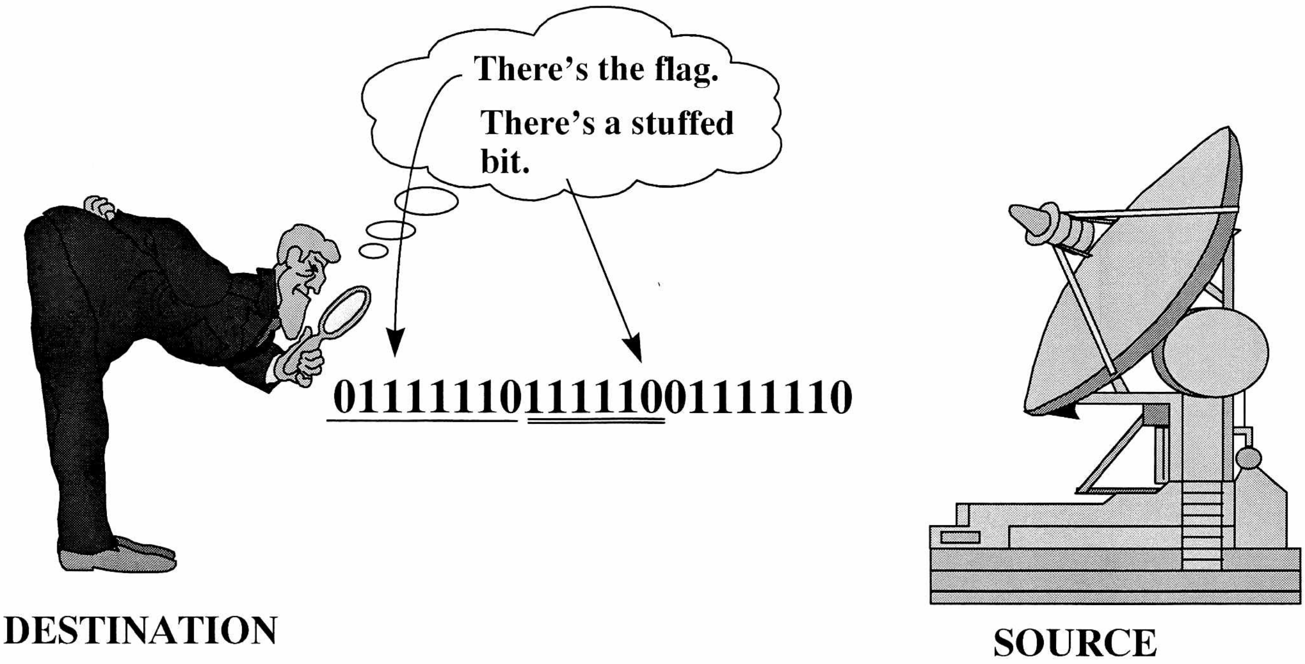
The **flag** sequence consists of 01111110. Flags are transmitted on the link between HDLC frames to keep the link active. As such, they are known as interframe signals.

At least seven, but fewer than 15 continuous 1s is an **abort** signal and indicates a problem on the link.

Fifteen or more 1s keep the channel **idle.** A station can detect the idle pattern and reverse the transmission direction.

To prevent "phony" flags from being inserted into the frame, the transmitter inserts a zero bit after it encounters five continuous 1s anywhere between the opening and closing flags of the frame. Zero insertion applies to the address, control, information, and FCS fields. This technique is called **bit stuffing**.

A Little Bit More



SNIFFER® UNIVERSITY

HDLC 6 - 11

Internetwork Analysis and Troubleshooting, 10/96, Rev. 5.0

Network General

Bit stuffing is used to prevent false flags from being inserted into the frame. If the transmitter detects five consecutive 1s anywhere between the beginning and ending flags, it inserts a 0 bit.

The receiver monitors the stream of bits and if a 0 is followed by five 1s, the next bit is inspected. If it is a 0, the stuffed bit is removed. If the seventh bit is a 1, the receiver inspects the eight bit. If a zero, the receiver knows it's a flag.

Fifteen or more 1s signal an idle condition. At least 7, but fewer than 15 1s signal an abort condition.

Idles may be sent following transmission in half-duplex mode (not supported in LAPB) to signal the other side to reverse the transmission line.

Addressing Conventions

- A unique address is associated with each station.
- In an unbalanced configuration, the address field for both commands and responses contains the address of the secondary.
- In a balanced configuration such as LAPB:
  - A station transmitting a **command** places the address of the receiving station in the address field.
  - A station transmitting a **response** places its own address in the address field.
  - X.25 specifies LAPB address fields <u>specifically</u> designate the DTE as 01 and the DCE as 03.

Therefore,
All commands **from**, and responses **to** the **DTE** are **01.**

All commands **from**, and responses **to** the **DCE** are **03.**

Station Transmitting a Command

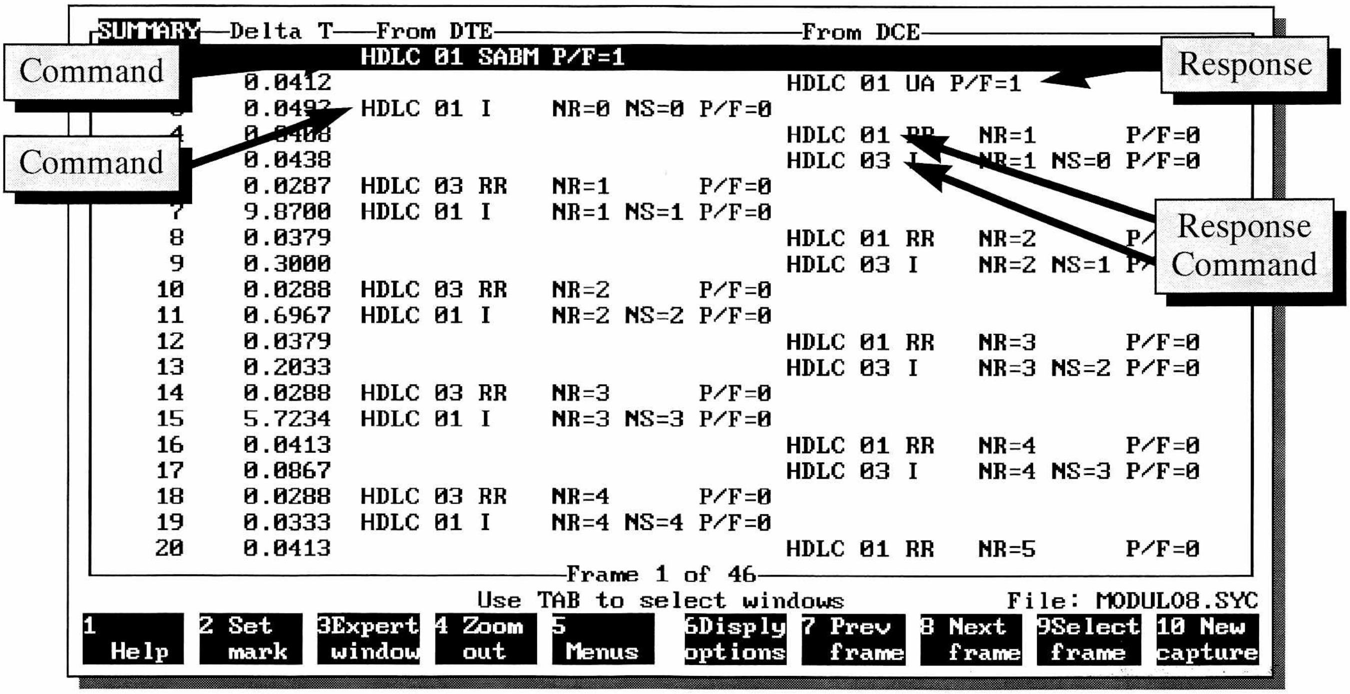
```
SUMMARY—Delta T—DST——————————————SRC———————————————————————————————————————————
M    1              DCE.HDLC.01      «DTE.HDLC.01     HDLC 01 SABM P/F=1
     2    0.0412    DTE.HDLC.01      «DCE.HDLC.01     HDLC 01 UA P/F=1
     3    0.0492    DCE.HDLC.01      «DTE.HDLC.01     HDLC 01 I    NR=0 NS=0 P/F
     4    0.0408    DTE.HDLC.01      «DCE.HDLC.01     HDLC 01 RR   NR=1      P/F
     5    0.0438    DTE.HDLC.03      «DCE.HDLC.03     HDLC 03 I    NR=1 NS=0 P/F
     6    0.0287    DCE.HDLC.03      «DTE.HDLC.03     HDLC 03 RR   NR=1      P/F
     7    9.8700    DCE.HDLC.01      «DTE.HDLC.01     HDLC 01 I    NR=1 NS=1 P/F
     8    0.0379    DTE.HDLC.01      «DCE.HDLC.01     HDLC 01 RR   NR=2      P/F
     9    0.3000    DTE.HDLC.03      «DCE.HDLC.03     HDLC 03 I    NR=2 NS=1 P/F
————————————————————————————————————Frame 1 of 46——————————————————————————————
DETAIL
 HDLC: ----- High Level Data Link Control (HDLC) -----
 HDLC:
 HDLC: Address = 01
 HDLC: Control field = 3F
 HDLC:      ...1 .... = Poll/Final bit
 HDLC:      001. 1111 = SABM (Set asynchronous balanced mode)
 HDLC:
————————————————————————————————————Frame 1 of 46——————————————————————————————
                               Use TAB to select windows           File: MODUL08.SYC
1       2 Set   3Expert  4 Zoom  5        6Disply  7 Prev  8 Next  9Sel ct  10 New
  Help    mark  window     in    Menus    options  frame   frame   fr  e    capture
```

Trace file name

Station Transmitting A Response

```
SUMMARY—Delta T—DST——————————————SRC————
M    1            DCE.HDLC.01     «DTE.HDLC.01      HDLC 01 SABM P/F=1
     2   0.0412   DTE.HDLC.01     «DCE.HDLC.01      HDLC 01 UA P/F=1
     3   0.0492   DCE.HDLC.01     «DTE.HDLC.01      HDLC 01 I    NR=0 NS=0 P/F
     4   0.0408   DTE.HDLC.01     «DCE.HDLC.01      HDLC 01 RR   NR=1      P/F
     5   0.0438   DTE.HDLC.03     «DCE.HDLC.03      HDLC 03 I    NR=1 NS=0 P/F
     6   0.0287   DCE.HDLC.03     «DTE.HDLC.03      HDLC 03 RR   NR=1      P/F
     7   9.8700   DCE.HDLC.01     «DTE.HDLC.01      HDLC 01 I    NR=1 NS=1 P/F
     8   0.0379   DTE.HDLC.01     «DCE.HDLC.01      HDLC 01 RR   NR=2      P/F
     9   0.3000   DTE.HDLC.03     «DCE.HDLC.03      HDLC 03 I    NR=2 NS=1 P/F
                                   ——————Frame 2 of 46——————
DETAIL
 DLC:  Source = DCE
 DLC:
 HDLC: ----- High Level Data Link Control (HDLC) -----
 HDLC:
 HDLC: Address = 01
 HDLC: Control field = 73
 HDLC:      ...1 .... = Poll/Final bit
 HDLC:      011. 0011 = UA (Unnumbered acknowledgement)
 HDLC:
                                   ——————Frame 2 of 46——————
                         Use TAB to select windows          File: MODUL08.SYC
1      2 Set  3Expert 4 Zoom 5       6Disply 7 Prev 8 Next 9Select 10 New
 Help   mark   window  in     Menus  options  frame  frame  frame  capture
```

Two-Station Format Display



HDLC Addressing Exercise

Objective: Study HDLC DTE/DCE addressing.

1. Load the file C:\SYCAP\TC107\HDLCFRAM.SYC. Turn on **Summary window**, **2-station format**, **HDLC protocol display filter**, **DLC addresses**.

   Look at the addresses in frames 1 and 2. Based on the addresses, is frame 2 the response to frame 1?

2. Now look at the addresses in frames 8 and 9. Is frame 9 the response to frame 8?

3. Which frame is the response to frame 8?

4. In the response to question 3, what is the DCE's HDLC address and what is the DTE's HDLC address?

HDLCFRAM Trace

```
┌SUMMARY──Delta T──DST──────────────SRC──────────────────────────────────────────────────────┐
│M    1            DCE              «DTE               HDLC C RR    NR=6       P/F=1          │
│     2   0.0331   DTE              «DCE               HDLC R RR    NR=3       P/F=1          │
│     3   0.1146   DCE.LCN.001      «DTE.LCN.001       HDLC C I     NR=6 NS=3  P/F=0          │
│     4   0.0067   DCE.LCN.008      «DTE.LCN.008       HDLC C I     NR=6 NS=4  P/F=0          │
│     5   0.0066   DCE.LCN.008      «DTE.LCN.008       HDLC C I     NR=6 NS=5  P/F=0          │
│     6   0.0083   DCE.LCN.008      «DTE.LCN.008       HDLC C I     NR=6 NS=6  P/F=0          │
│     7   0.0137   DTE              «DCE               HDLC R RR    NR=4       P/F=0          │
│     8   0.0067   DTE.LCN.001      «DCE.LCN.001       HDLC C I     NR=4 NS=6  P/F=0          │
│     9   0.0042   DTE              «DCE               HDLC R RR    NR=5       P/F=0          │
└───────────────────────────────────Frame 8 of 14──────────────────────────────────────────────┘
┌DETAIL──────────────────────────────────────────────────────────────────────────────────────┐
│ HDLC: ----- High Level Data Link Control (HDLC) -----                                       │
│ HDLC:                                                                                       │
│ HDLC: Address = 03 (Command)                                                                │
│ HDLC: Control field = 8C                                                                    │
│ HDLC:     100. .... = N(R) = 4                                                              │
│ HDLC:     ...0 .... = Poll/Final bit                                                        │
│ HDLC:     .... 110. = N(S) = 6                                                              │
│ HDLC:     .... ...0 = I (Information transfer)                                              │
│ HDLC:                                                                                       │
└───────────────────────────────────Frame 8 of 14──────────────────────────────────────────────┘
                               Use TAB to select windows               File: HDLCFRAM.SYC
1       2 Set   3Expert 4 Zoom  5        6Disply 7 Prev  8 Next  9Select 10 New
  Help    mark  window    in      Menus  options   frame   frame frame   capture
```

HDLCFRAM Trace

Continued

```
SUMMARY—Delta T—DST————————————SRC——————————————————————————————————————————————
     3   0.1146  DCE.LCN.001  «DTE.LCN.001       HDLC C I     NR=6 NS=3 P/F=0
     4   0.0067  DCE.LCN.008  «DTE.LCN.008       HDLC C I     NR=6 NS=4 P/F=0
     5   0.0066  DCE.LCN.008  «DTE.LCN.008       HDLC C I     NR=6 NS=5 P/F=0
     6   0.0083  DCE.LCN.008  «DTE.LCN.008       HDLC C I     NR=6 NS=6 P/F=0
     7   0.0137  DTE          «DCE               HDLC R RR    NR=4      P/F=0
     8   0.0067  DTE.LCN.001  «DCE.LCN.001       HDLC C I     NR=4 NS=6 P/F=0
     9   0.0042  DTE          «DCE               HDLC R RR    NR=5      P/F=0
    10   0.0071  DCE          «DTE               HDLC R RR    NR=7      P/F=0
    11   0.1015  DTE.LCN.008  «DCE.LCN.008       HDLC C I     NR=5 NS=7 P/F=0
————————————————————————————————————Frame 9 of 14———————————————————————————————
DETAIL——————————————————————————————————————————————————————————————————————————
  DLC:
  HDLC: ----- High Level Data Link Control (HDLC) -----
  HDLC:
  HDLC: Address = 01 (Response)
  HDLC: Control field = A1
  HDLC:     101. .... = N(R) = 5
  HDLC:     ...0 .... = Poll/Final bit
  HDLC:     .... 0001 = RR  (Receive ready)
  HDLC:
————————————————————————————————————Frame 9 of 14———————————————————————————————
                              Use TAB to select windows          File: HDLCFRAM.SYC
1        2 Set    3Expert  4 Zoom   5                 6Disply  7 Prev   8 Next   9Select  10 New
  Help     mark    window    in      Menus            options   frame    frame    frame   capture
```


HDLC 6 - 18

HDLCFRAM Trace

Continued

```
SUMMARY—Delta T—DST————————————SRC——————————————————————————————————————————————
      2    0.0331  DTE            «DCE              HDLC R RR    NR=3        P/F=1
      3    0.1146  DCE.LCN.001    «DTE.LCN.001      HDLC C I     NR=6 NS=3   P/F=0
      4    0.0067  DCE.LCN.008    «DTE.LCN.008      HDLC C I     NR=6 NS=4   P/F=0
      5    0.0066  DCE.LCN.008    «DTE.LCN.008      HDLC C I     NR=6 NS=5   P/F=0
      6    0.0083  DCE.LCN.008    «DTE.LCN.008      HDLC C I     NR=6 NS=6   P/F=0
      7    0.0137  DTE            «DCE              HDLC R RR    NR=4        P/F=0
      8    0.0067  DTE.LCN.001    «DCE.LCN.001      HDLC C I     NR=4 NS=6   P/F=0
      9    0.0042  DTE            «DCE              HDLC R RR    NR=5        P/F=0
     10    0.0071  DCE            «DTE              HDLC R RR    NR=7        P/F=0
————————————————————————————————————Frame 10 of 14——————————————————————————————
DETAIL
 DLC:
 HDLC: ----- High Level Data Link Control (HDLC) -----
 HDLC:
 HDLC: Address = 03 (Response)
 HDLC: Control field = E1
 HDLC:      111. .... = N(R) = 7
 HDLC:      ...0 .... = Poll/Final bit
 HDLC:      .... 0001 = RR  (Receive ready)
 HDLC:
————————————————————————————————————Frame 10 of 14——————————————————————————————
                                Use TAB to select windows         File: HDLCFRAM.SYC
1       2 Set   3Expert 4 Zoom  5       6Disply 7 Prev  8 Next  9Select 10 New
 Help    mark   window   in     Menus   options  frame   frame   frame  capture
```

HDLCFRAM Trace

Continued

```
┌SUMMARY─Delta T─DST──────────SRC───┐ ┌SUMMARY─Delta T─DST──────────SRC───┐
│      6   0.0083  DCE.LCN.008  «DTE.L│ │      6   0.0083  DCE.LCN.008  «DTE.L│
│      7   0.0137  DTE          «DCE  │ │      7   0.0137  DTE          «DCE  │
│      8   0.0067  DTE.LCN.001  «DCE.L│ │      8   0.0067  DTE.LCN.001  «DCE.L│
│      9   0.0042  DTE          «DCE  │ │      9   0.0042  DTE          «DCE  │
│     10   0.0071  DCE          «DTE  │ │     10   0.0071  DCE          «DTE  │
│     11   0.1015  DTE.LCN.008  «DCE.L│ │     11   0.1015  DTE.LCN.008  «DCE.L│
│     12   0.0042  DTE          «DCE  │ │     12   0.0042  DTE          «DCE  │
│     13   0.0042  DTE          «DCE  │ │     13   0.0042  DTE          «DCE  │
│     14   0.0067  DTE.LCN.008  «DCE.L│ │     14   0.0067  DTE.LCN.008  «DCE.L│
└────────────Frame 8 of 14────────────┘ └────────────Frame 10 of 14───────────┘
┌DETAIL──────────────────────────────┐ ┌DETAIL──────────────────────────────┐
│ HDLC: ----- High Level Data Link Con│ │ DLC:                               │
│ HDLC:                               │ │ HDLC: ----- High Level Data Link Con│
│ HDLC: Address = 03 (Command)        │ │ HDLC:                              │
│ HDLC: Control field = 8C            │ │ HDLC: Address = 03 (Response)      │
│ HDLC:     100. .... = N(R) = 4      │ │ HDLC: Control field = E1           │
│ HDLC:     ...0 .... = Poll/Final bit│ │ HDLC:     111. .... = N(R) = 7     │
│ HDLC:     .... 110. = N(S) = 6      │ │ HDLC:     ...0 .... = Poll/Final bit│
│ HDLC:     .... ...0 = I (Information│ │ HDLC:     .... 0001 = RR  (Receive r│
│ HDLC:                               │ │ HDLC:                              │
└────────────Frame 8 of 14────────────┘ └────────────Frame 10 of 14───────────┘
                          Use TAB to select windows          File: HDLCFRAM.SYC
 1       2 Set   3Expert  4 Zoom  5        6Disply  7 Prev  8 Next  9Select  10 New
  Help    mark    window   in      Menus   options   frame   frame   frame   capture
```


HDLC 6 - 20

Take Control - 3 HDLC Frame Types

- **Unnumbered frames:**
  - Establish link connections/disconnections
  - Provide link maintenance and error recovery
  - Provide connectionless (datagram) support (IEEE 802.2 LLC Type 1 only)

- **Supervisory frames:**
  - Acknowledge frames received
  - Request retransmission of frame(s)
  - Provide flow control

- **Information frames:**
  - Transport user data and higher layer protocols
  - Increment sequence numbers

Unnumbered (U) frames are used to initialize and tear down the link, select either a one or a two byte control field, and perform other SDLC data link layer maintenance and control functions. Unnumbered frames are not sequenced.

Supervisory frames contain information designed to control data flow, report status, and acknowledge information frames.

Information frames carry upper-layer data and also perform some control functions.

Supervisory Frame Types

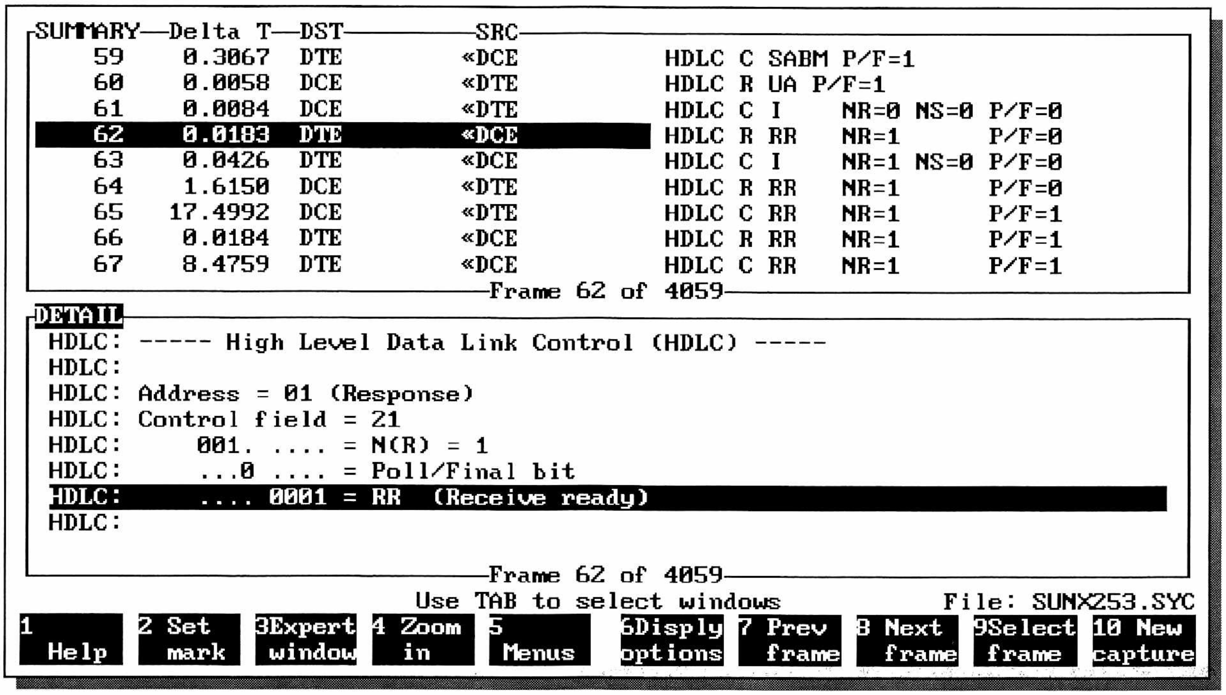
Sniffer Summary	Type	Command/ Response	Function
RR	Receive Ready	C/R	Can accept data
RNR	Receive Not Ready	C/R	Cannot accept data
REJ	Reject	C/R	Negative ack - go back to **N**

Information Frame

I	Information	C/R	Data

REJ are caused by receipt of a out of sequence frame or FCS error.

Receive Ready (RR)



Frame 64 shows the first RR.

The **Receive Ready (RR)** frame is to indicate that is ready to receive an information frame and/or acknowledge previously received frames. The primary station may also use the receive ready command to poll a secondary station by setting the P bit to 1.

Receive Not Ready (RNR)

```
SUMMARY—Delta T—DST————————SRC——————————————————————————————————————————
  77  10.6427  DCE         «DTE         HDLC C SABM P/F=1
  78   0.0248  DTE         «DCE         HDLC R UA P/F=1
  79   0.0042  DTE         «DCE         HDLC R RNR  NR=0        P/F=0
  80   0.0042  DTE         «DCE         HDLC R RR   NR=0        P/F=0
  81   0.0036  DCE         «DTE         HDLC C I    NR=0 NS=0 P/F=0
  82   0.0180  DTE         «DCE         HDLC R RR   NR=1        P/F=0
  83   0.0184  DTE         «DCE         HDLC C I    NR=1 NS=0 P/F=0
  84   1.7777  DCE         «DTE         HDLC R RR   NR=1        P/F=0
  85   8.3326  4152574300 «4152574300  HDLC C I    NR=1 NS=1 P/F=0
——————————————————————————————Frame 79 of 4059——————————————————————————
DETAIL——————————————————————————————————————————————————————————————————
 DLC:
 HDLC: ----- High Level Data Link Control (HDLC) -----
 HDLC:
 HDLC: Address = 01 (Response)
 HDLC: Control field = 05
 HDLC:       000. .... = N(R) = 0
 HDLC:       ...0 .... = Poll/Final bit
 HDLC:       .... 0101 = RNR (Receive not ready)
 HDLC:
——————————————————————————————Frame 79 of 4059——————————————————————————
                          Use TAB to select windows         File: SUNX253.SYC
1      2 Set  3Expert 4 Zoom  5       6Disply 7 Prev  8 Next  9Select 10 New
 Help   mark   window   in     Menus  options  frame   frame   frame  capture
```


Frame 79 shows the first RNR.

The **Receive Not Ready (RNR)** frame is used by a station to inform the transmitting station that it cannot accept additional incoming data. A temporary busy condition and the inability to accept further I-frames (as with buffer depletion), is communicated by sending Receive Not Ready (RNR) commands.

Reject (REJ)

```
SUMMARY—Delta T——From DTE————————————————From DCE——————————————————————
    32    0.0958                         HDLC C I    NR=3 NS=2 P/F=0
    33    0.0102  HDLC C I    NR=2 NS=3 P/F=0
    34    0.0714                         HDLC C I    NR=4 NS=3 P/F=0
    35    0.0348  HDLC C I    NR=3 NS=4 P/F=0
    36    0.1019                         HDLC retransmission
                                         HDLC C I    NR=5 NS=5 P/F=0
    37    0.0090  REJ reject
                  HDLC C REJ  NR=4      P/F=0
    38    0.1051                         HDLC C I    NR=5 NS=4 P/F=0
————————————————————————————————Frame 37 of 38——————————————————————————
DETAIL
 HDLC: ----- High Level Data Link Control (HDLC) -----
 HDLC:
 HDLC: Address = 01 (Command)
 HDLC: Control field = 89
 HDLC:     100. .... = N(R) = 4
 HDLC:     ...0 .... = Poll/Final bit
 HDLC:     .... 1001 = REJ (Reject)
 HDLC:
————————————————————————————————Frame 37 of 38——————————————————————————
                           Use TAB to select windows          File: xx25call.SYC
1      2 Set  3Expert 4 Zoom 5       6Disply 7 Prev 8 Next 9Select 10 New
 Help   mark  window   in    Menus  options  frame  frame  frame  capture
```

SNIFFER® UNIVERSITY

HDLC 6 - 25

Internetwork Analysis and Troubleshooting, 10/96, Rev. 5.0

Network General

The **Reject (REJ)** is used to request retransmission of frames starting with the frame numbered in the N(R) field. Frames numbered N(R) - 1 are all acknowledged. The REJ frame can be used to implement the go-back-N technique.

Information Frame

```
SUMMARY—Delta T——From DTE——————————————From DCE——————————————————
     27     0.0550  HDLC C I    NR=7 NS=0 P/F=0
     28     0.0642                           HDLC C I    NR=1 NS=0 P/F=0
     29     0.0417  HDLC C I    NR=0 NS=1 P/F=0
     30     0.0775                           HDLC C I    NR=2 NS=1 P/F=0
     31     0.0283  HDLC C I    NR=1 NS=2 P/F=0
     32     0.0958                           HDLC C I    NR=3 NS=2 P/F=0
     33     0.0102  HDLC C I    NR=2 NS=3 P/F=0
     34     0.0714                           HDLC C I    NR=4 NS=3 P/F=0
     35     0.0348  HDLC C I    NR=3 NS=4 P/F=0
——————————————————————————Frame 31 of 38——————————————————————————
DETAIL
 HDLC:
 HDLC: Address = 01 (Command)
 HDLC: Control field = 24
 HDLC:     001. .... = N(R) = 1
 HDLC:     ...0 .... = Poll/Final bit
 HDLC:     .... 010. = N(S) = 2
 HDLC:     .... ...0 = I (Information transfer)
 HDLC:
 X.25: ----- X.25 Packet Level -----
——————————————————————————Frame 31 of 38——————————————————————————
                    Use TAB to select windows            File: xx25call.SYC
1        2 Set   3Expert 4 Zoom  5        6Disply 7 Prev  8 Next  9Select 10 New
 Help     mark   window   in      Menus   options  frame   frame   frame  capture
```

SNIFFER® UNIVERSITY

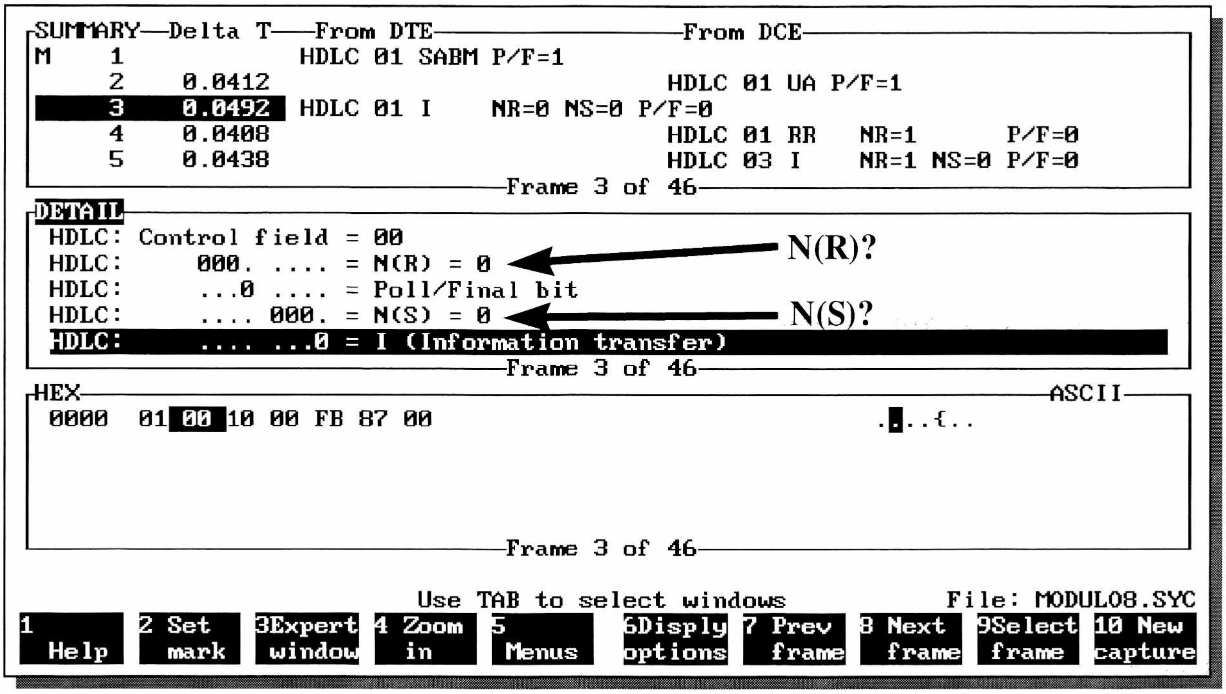
HDLC 6 - 26

Internetwork Analysis and Troubleshooting, 10/96, Rev. 5.0

Demonstration file: C:\SYCAP\TC107\UNSUPINF.SYC

The **Information field (I field)** contains the actual user data. It resides only in frames in the information frame format. Usually, it is not found in supervisory or unnumbered frames, although one option of HDLC allows the I field to be used with an unnumbered frame. With LAPB, the I field contains the X.25 packet.

What's N(R) and N(S)?



I-frames are assigned pairs of sequence numbers that operate in both send and receive directions and insure that no frames are lost or sent out of order. Each transmitted frame is given a frame sequence number. The **N(S)** field is used to identify the sequence numbers and is advanced by 1 for each frame sent.

The receiver maintains as **N(R)** its own account of error-free frames received. Each time an error-free frame is received, the N(R) count is incremented to the sequence number of the next expected frame. Acknowledgments of correctly received frames flow back to the sender imbedded in frames sent by the receiver and indicated in the receiver's own N(R) count. As long as both sender and receiver pass I_frames, no separate explicit acknowledgment frames are required.

Decoding HDLC Frames

From DTE.HDLC.01	HDLC 01 SABM P/F=1
01	Address of DCE (Command)
SABM	Initialize session, using Modulo 8 window
P/F=1	Poll bit is set; DTE expects a response from DCE.

From DCE.HDLC.01	HDLC 01 UA P/F=1
01	Address of DCE (Response)
UA	Unnumbered Acknowledgment
P/F=1	Final bit is set; response to DTE's poll.

From DTE.HDLC.01	HDLC 01 I NR=0 NS=0 P/F=0
01	Address of DCE (Command)
I	Information frame; higher layer data included
NR=0	DTE **N**ext expects to **R**eceive frame 0
NS=0	DTE is **N**ow **S**ending frame 0
P/F=0	Poll/Final bit is not set.

NR=1
ACKs
NS=0

From DCE.HDLC.01	HDLC 01 RR NR=1 P/F=0
01	Address of DCE (Response)
RR	Receive Ready; ready to receive data
NR=1	Next frame DCE expects to receive is frame 1
P/F=0	Poll/Final bit not set.

From DCE.HDLC.03	HDLC 03 I NR=1 NS=0
03	Address of DTE (DCE giving the Command)
I	Information frame
NR=1	DCE still expecting frame 1 next
NS=0	DCE now sending first sequenced frame 0.

From DTE.HDLC.03	HDLC 03 RR NR=1
03	Address of DTE (Response)
RR	Receive Ready
NR=1	DTE expects frame 1 next.

Also an ACK

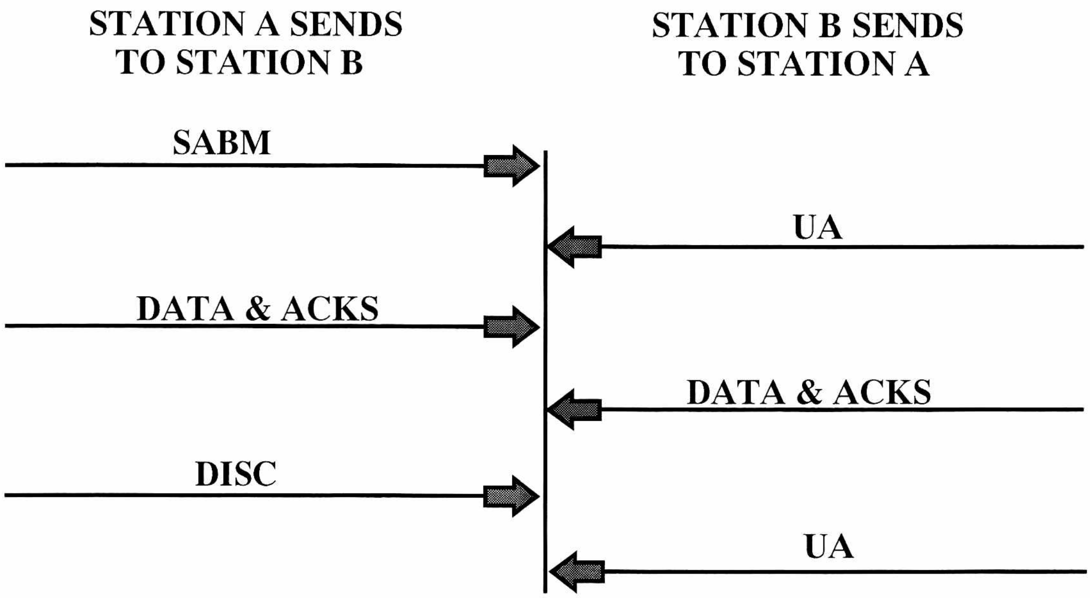
MODUL08.SYC

An easy way to remember **NS** and **NR** is:

NS means **N**ow **S**ending

NR means **N**ext to **R**eceive

Link Setup and Disconnect



SNIFFER® UNIVERSITY

HDLC 6 - 29

Internetwork Analysis and Troubleshooting, 10/96, Rev. 5.0

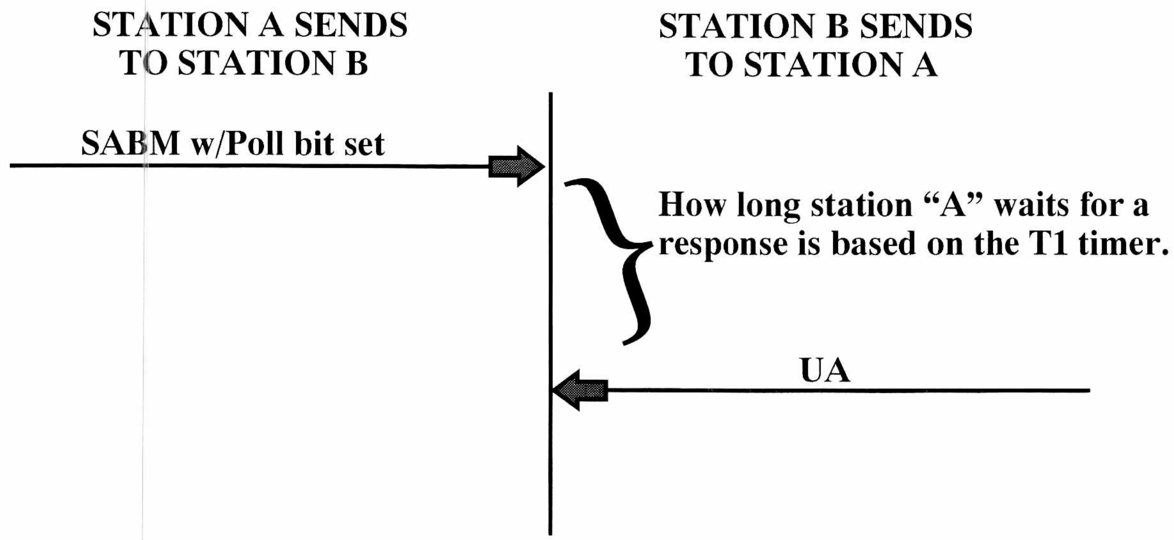
Network General

Either station can establish the link. A station indicates it is able to set up the link by transmitting continuous flags. Before link setup, either station can send DISC to make certain all traffic and modes are cleared. If the link cannot be set up, DM must be returned.

If the receiving station accepts the SABM/SABME, it sends back a UA frame. Upon receipt of the UA, the station resets its send and receive state variables to zero, and stops the T1 timer. The link is then ready for traffic. The link will not accept any other frames after issuing the link-setup commands except another SABM/SABME, UA, or DM.

A station can disconnect the link at any time by issuing the DISC command. UA is the expected response. After entering the disconnect phase, a station may initiate link setup again. If the initiation is successful, the UA is returned.

HDLC Timers



HDLC defines two timers: T1 and T2. Most implementations use T1 in some fashion. T2 is used, but not as frequently as T1. LAPB also defines a third timer called T3. The timers are used as follows:

T1: A primary station sends a frame and checks to see of a response to the P bit is received within a defined time. This function is controlled by the timer T1 and is called the "wait for F" time-out.

T2: T2 is set to the amount of time available at the DTE or network before an acknowledging frame must be sent.

T3: In LAPB, T3 is used to signify to the network layer that excessively long idle time is occurring on the link. LAPB requires that T3 > T1.

Unnumbered Frame Types

Sniffer Summary	Type	Command/ Response	Function
SABME	Set Asynchronous Balanced Mode Extended	C	Sets mode to ABM in which both stations are peers. Window size is extended to 127.
UA	Unnumbered Acknowledgment	R	Acknowledge acceptance of a SABME or a DISC.
DISC	Disconnect	C	Initiate disconnection. Normal response is UA.
DM	Disconnect Mode	R	Informs primary that the secondary is in a logically disconnected state.
FRMR	Frame Reject	R	Report an error condition; a response to a command to perform an unsupported action.
XID	Exchange Identification	C/R	Used to request/report status.
TEST	Test	C/R	Exchange identical information field for testing.
UI	Unnumbered Information	C/R	Allows for connectionless-mode service. Used in IEEE 802.2 Logical Link Control.

A FRMR causes a reset of the data link. It is usually answered with a DISC frame. The FRMR always contains a 3-byte diagnostic field immediately following the FRMR's control field, that explains why it was sent. For example:

- Receipt of a I frame with I field too long.
- Receipt of a command or response that is invalid or not implemented.

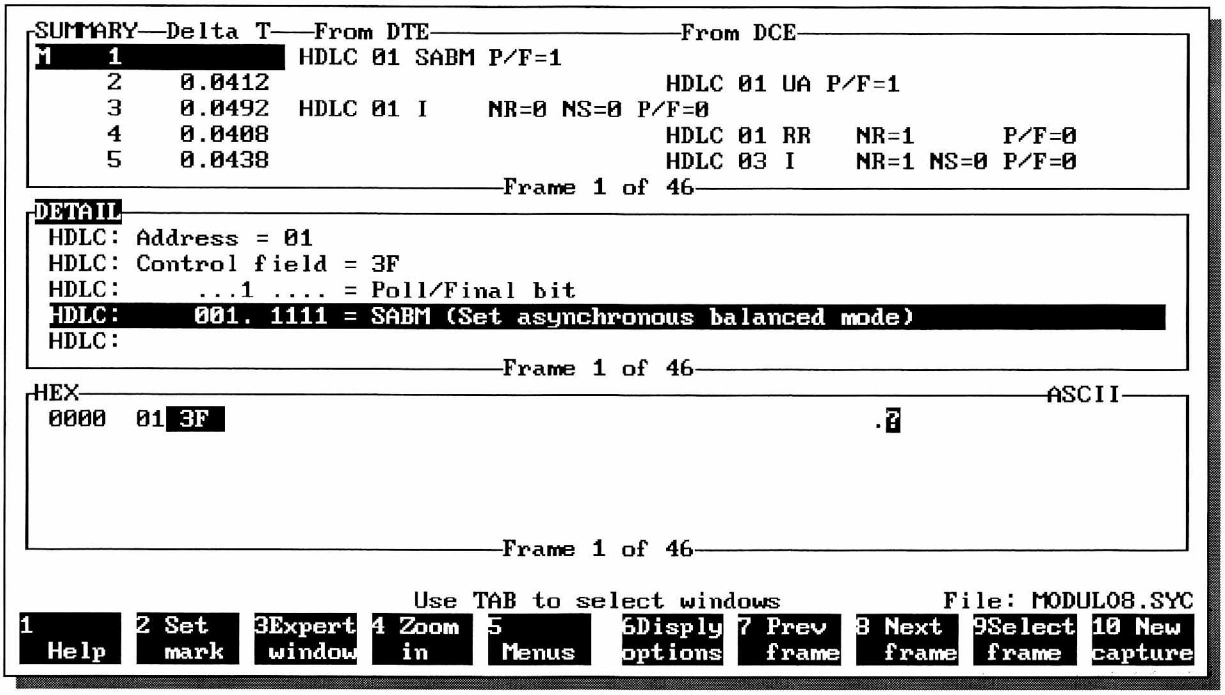
Unnumbered Frame

```
SUMMARY  Delta T   From DTE                      From DCE
M    1             HDLC 01 SABM P/F=1
     2   0.0412                                  HDLC 01 UA P/F=1
     3   0.0492    HDLC 01 I    NR=0 NS=0 P/F=0
     4   0.0408                                  HDLC 01 RR    NR=1        P/F=0
     5   0.0438                                  HDLC 03 I     NR=1 NS=0 P/F=0
                                 Frame 2 of 46
DETAIL
  HDLC: Address = 01
  HDLC: Control field = 73
  HDLC:      ...1 .... = Poll/Final bit
  HDLC:     011. 0011 = UA (Unnumbered acknowledgement)
  HDLC:
                                 Frame 2 of 46
HEX                                                                  ASCII
 0000   01 73                                                 .s



                                 Frame 2 of 46

                       Use TAB to select windows          File: MODULO8.SYC
1        2 Set   3Expert 4 Zoom  5        6Disply 7 Prev  8 Next  9Select 10 New
  Help     mark   window   in     Menus   options  frame   frame   frame  capture
```


Demonstration file: C:\SYCAP\TC107\UNSUPINF.SYC Unnumbered frames are used to initialize and tear down the link, select either a one or two byte control field, and perform other HDLC data link layer maintenance and control functions. Unnumbered frames lead off with two 1 bits, which identify the frame as an unnumbered frame. Following this are two function code bits, a P/F bit, and three more function code bits. Unnumbered frames are not sequenced.

Unnumbered Information (UI) format allows for transmission of user data in an unnumbered frame. The UI frame is actually a form of connectionless-mode protocol; the absence of the N(S) and N(R) fields precludes flow controlling and acknowledging frames. The IEEE 802.2 Logical Link Control protocol uses this approach with LLC type 1 version of HDLC.

Set Asynchronous Balanced Mode (SABM)



Frame 165 shows a SABM followed by a DM. Frame 174 shows a SABM followed by a UA.

LAPB treats DTE and DCE as equals (no master/slave relation). Since this is a balanced link access procedure, either end can begin link initialization by sending out the SABM (Set Asynchronous Balanced Mode) command. The acceptance of the SABM is confirmed by the other (receiving) side when it issues a UA (Unnumbered Ack).

SABMs use a modulo 8 window - (sequence numbers are from 0 through 7).

LAPB started using extended sequencing in 1984 to accommodate the need for additional outstanding frames in satellite and optical links, due to the long transit time of the link.

The SABME uses a modulo 128 window (sequence numbers from 0-127).

Unnumbered Acknowledgment (UA)

```
SUMMARY—Delta T—DST———————————SRC—
 163     2.0023  DTE.HDLC.03     «DCE.HDLC.03        HDLC disconnect
                                                     HDLC 03 DISC P/F=0
 164     0.0034  DCE.HDLC.03     «DTE.HDLC.03        HDLC 03 UA P/F=0
 165     0.0019  DCE.HDLC.01     «DTE.HDLC.01        HDLC 01 SABM P/F=0
 166     0.0054  DTE.HDLC.01     «DCE.HDLC.01        HDLC 01 DM P/F=0
 167     3.0105  DCE.HDLC.01     «DTE.HDLC.01        HDLC 01 SABM P/F=1
 168     0.0033  DTE.HDLC.01     «DCE.HDLC.01        HDLC 01 DM P/F=1
 169     0.0028  DCE.HDLC.01     «DTE.HDLC.01        HDLC 01 SABM P/F=0
 170     0.0029  DTE.HDLC.01     «DCE.HDLC.01        HDLC 01 DM P/F=0
                               Frame 163 of 200
DETAIL
 DLC:   Source = DCE
 DLC:
 HDLC:  ----- High Level Data Link Control (HDLC) -----
 HDLC:
 HDLC:  Address = 03
 HDLC:  Control field = 43
 HDLC:      ...0 .... = Poll/Final bit
 HDLC:      010. 0011 = DISC (Disconnect)
 HDLC:
                               Frame 163 of 200
                     Use TAB to select windows            File: BRGVTX25.SYC
1       2 Set  3Expert 4 Zoom 5        6Disply 7 Prev 8 Next 9Select 10 New
  Help    mark  window   in     Menus  options  frame  frame  frame  capture
```

SNIFFER® UNIVERSITY

HDLC 6 - 34

Internetwork Analysis and Troubleshooting, 10/96, Rev. 5.0

Network General

The **Unnumbered Acknowledgment (UA)** frame is used in two different ways:

1. Clears a busy condition. Proper response to RNR or DM.
2. Received mode setting command are not acted upon until UA is transmitted. Proper response to SABM/SABME.

Disconnect (DISC)

```
SUMMARY—Delta T—DST————————SRC————————
   163    2.0023  DTE.HDLC.03    «DCE.HDLC.03     HDLC disconnect
                                                  HDLC 03 DISC P/F=0
   164    0.0034  DCE.HDLC.03    «DTE.HDLC.03     HDLC 03 UA P/F=0
   165    0.0019  DCE.HDLC.01    «DTE.HDLC.01     HDLC 01 SABM P/F=0
   166    0.0054  DTE.HDLC.01    «DCE.HDLC.01     HDLC 01 DM P/F=0
   167    3.0105  DCE.HDLC.01    «DTE.HDLC.01     HDLC 01 SABM P/F=1
   168    0.0033  DTE.HDLC.01    «DCE.HDLC.01     HDLC 01 DM P/F=1
   169    0.0028  DCE.HDLC.01    «DTE.HDLC.01     HDLC 01 SABM P/F=0
   170    0.0029  DTE.HDLC.01    «DCE.HDLC.01     HDLC 01 DM P/F=0
                               ——————Frame 163 of 200——————
DETAIL
 DLC:   Source = DCE
 DLC:
 HDLC: ----- High Level Data Link Control (HDLC) -----
 HDLC:
 HDLC: Address = 03
 HDLC: Control field = 43
 HDLC:     ...0 .... = Poll/Final bit
 HDLC:     010. 0011 = DISC (Disconnect)
 HDLC:
                               ——————Frame 163 of 200——————
                          Use TAB to select windows         File: BRGVTX25.SYC
1      2 Set  3Expert 4 Zoom  5       6Disply 7 Prev  8 Next  9Select 10 New
 Help   mark  window   in     Menus  options  frame   frame   frame   capture
```


Frame 163 shows a DISC.

The **Disconnect (DISC)** places the secondary station in the disconnected mode. This command is valuable for switched lines: it provides a function similar to hanging up the telephone. UA is the expected response.

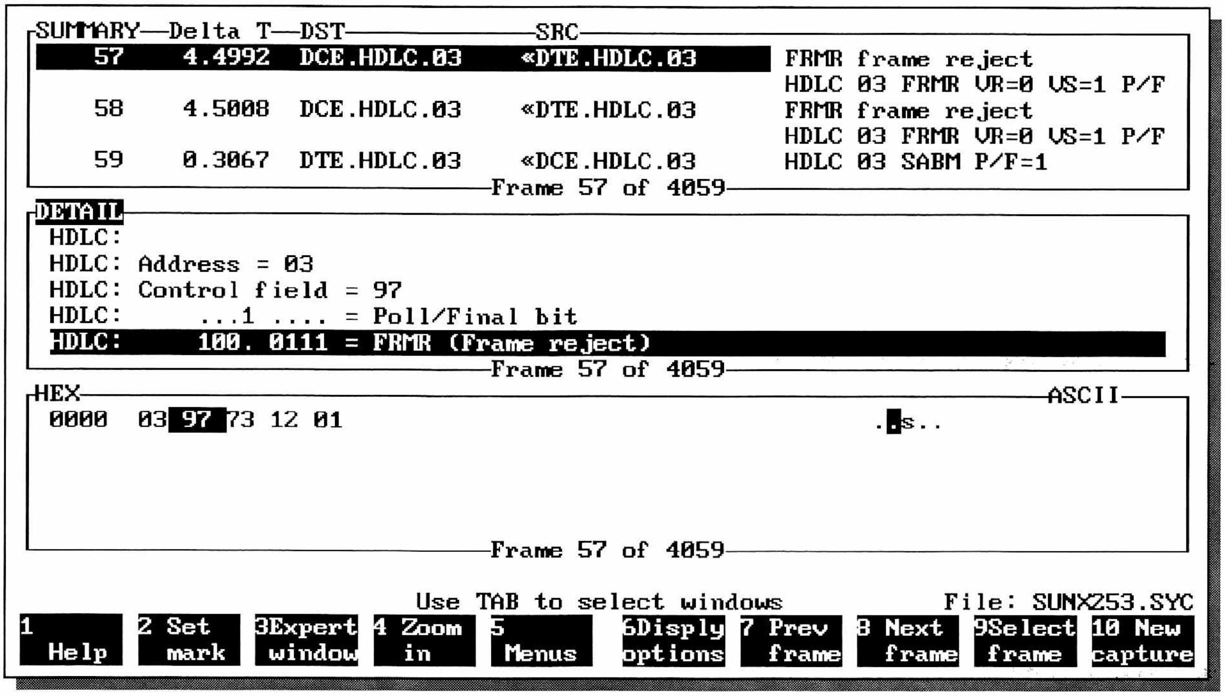
Disconnect Mode (DM)

```
SUMMARY—Delta T—DST—————————————SRC——————————————————————————————
   163   2.0023  DTE.HDLC.03    «DCE.HDLC.03      HDLC disconnect
                                                  HDLC 03 DISC P/F=0
   164   0.0034  DCE.HDLC.03    «DTE.HDLC.03      HDLC 03 UA P/F=0
   165   0.0019  DCE.HDLC.01    «DTE.HDLC.01      HDLC 01 SABM P/F=0
   166   0.0054  DTE.HDLC.01    «DCE.HDLC.01      HDLC 01 DM P/F=0
   167   3.0105  DCE.HDLC.01    «DTE.HDLC.01      HDLC 01 SABM P/F=1
   168   0.0033  DTE.HDLC.01    «DCE.HDLC.01      HDLC 01 DM P/F=1
   169   0.0028  DCE.HDLC.01    «DTE.HDLC.01      HDLC 01 SABM P/F=0
   170   0.0029  DTE.HDLC.01    «DCE.HDLC.01      HDLC 01 DM P/F=0
——————————————————————————————Frame 166 of 200———————————————————
DETAIL
 DLC:   Source = DCE
 DLC:
 HDLC:  ----- High Level Data Link Control (HDLC) -----
 HDLC:
 HDLC:  Address = 01
 HDLC:  Control field = 0F
 HDLC:      ...0 .... = Poll/Final bit
 HDLC:      000. 1111 = DM (Disconnected mode)
 HDLC:
——————————————————————————————Frame 166 of 200———————————————————
                           Use TAB to select windows        File: BRGVTX25.SYC
1      2 Set  3Expert 4 Zoom 5       6Disply 7 Prev 8 Next 9Select 10 New
 Help   mark   window   in    Menus  options  frame  frame  frame  capture
```


Frame 166 shows the first DM.

The **Disconnect Mode (DM)** is transmitted from a secondary station to indicate it is not operational. Also can be sent with or without a preceding DISC command.

Frame Reject (FRMR)



```
SUMMARY  Delta T  DST              SRC
   57    4.4992   DCE.HDLC.03      «DTE.HDLC.03    FRMR frame reject
                                                   HDLC 03 FRMR VR=0 VS=1 P/F
   58    4.5008   DCE.HDLC.03      «DTE.HDLC.03    FRMR frame reject
                                                   HDLC 03 FRMR VR=0 VS=1 P/F
   59    0.3067   DTE.HDLC.03      «DCE.HDLC.03    HDLC 03 SABM P/F=1
                               Frame 57 of 4059
DETAIL
 HDLC:
 HDLC: Address = 03
 HDLC: Control field = 97
 HDLC:       ...1 .... = Poll/Final bit
 HDLC:       100. 0111 = FRMR (Frame reject)
                               Frame 57 of 4059
HEX                                                         ASCII
 0000   03 97 73 12 01                                  ..s..
                               Frame 57 of 4059
                        Use TAB to select windows          File: SUNX253.SYC
1      2 Set  3Expert 4 Zoom  5      6Disply 7 Prev  8 Next  9Select 10 New
 Help   mark  window   in     Menus  options  frame   frame   frame  capture
```

SNIFFER® UNIVERSITY

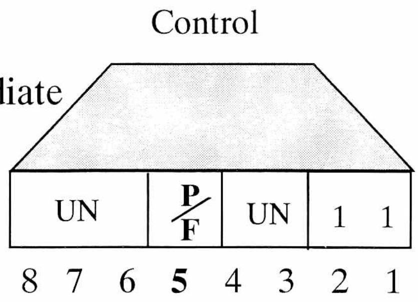
HDLC 6 - 37

Internetwork Analysis and Troubleshooting, 10/96, Rev. 5.0

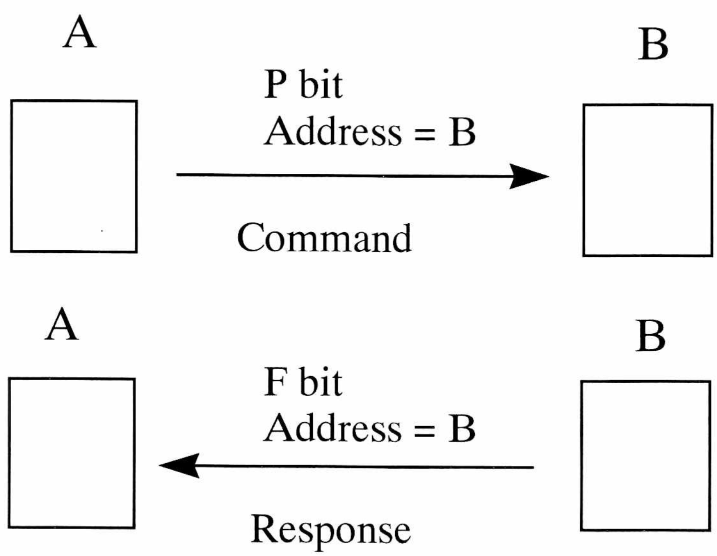
Network General

Unrecoverable errors, such as those not corrected by the retransmission of identical frames, are indicated with a **Frame Reject (FRMR)** response. Contained within this response are bit fields that indicate the specific reason for the rejection of a particular frame. Among the possible reasons are receipt of an undefined frame or invalid N(R) sequence numbers or information fields that exceed maximum established sizes.

The Poll/Final Bit



- The 5th bit in the control field is called the P/F bit.
- Recognized only when set to 1.
- The primary sets the P bit = 1 to request an immediate response from the secondary. LAPB uses the P bit to request a status and not an I frame.
- The secondary responds with a status frame (RR, RNR, etc.) with the F bit = 1 LABP only permits an unnumbered or supervisory frame be sent back.
- LAPB permits only one P bit to be outstanding at a time.



The Poll Bit

```
SUMMARY—Delta T—DST——————————————SRC——————————————————————————————————————————
   95  17.4994  DCE              «DTE               HDLC C RR   NR=4      P/F=1
   96   0.0182  DTE              «DCE               HDLC R RR   NR=4      P/F=1
   97   8.4760  DTE              «DCE               HDLC C RR   NR=4      P/F=1
   98   0.0068  DCE              «DTE               HDLC R RR   NR=4      P/F=1
   99   2.4201  2156901044       «031344152574301   HDLC C I    NR=4 NS=4 P/F=0
  100   0.0181  DTE              «DCE               HDLC R RR   NR=5      P/F=0
  101   0.5892  031344152574301«2156901044          HDLC C I    NR=5 NS=4 P/F=0
  102   0.0260  2156901044       «031344152574301   HDLC C I    NR=5 NS=5 P/F=0
  103   0.0181  DTE              «DCE               HDLC R RR   NR=6      P/F=0
————————————————————————————————Frame 95 of 4059——————————————————————————————
DETAIL
 HDLC: ----- High Level Data Link Control (HDLC) -----
 HDLC:
 HDLC: Address = 01 (Command)
 HDLC: Control field = 91
 HDLC:      100. .... = N(R) = 4
 HDLC:      ...1 .... = Poll/Final bit
 HDLC:      .... 0001 = RR  (Receive ready)
 HDLC:
————————————————————————————————Frame 95 of 4059——————————————————————————————
                              Use TAB to select windows          File: SUNX253.SYC
1        2 Set  3Expert 4 Zoom 5       6Disply 7 Prev 8 Next 9Select 10 New
   Help    mark  window   in    Menus  options  frame  frame  frame  capture
```


Frames 1 and 2 have the P/F bit set.

The Final Bit

```
SUMMARY--Delta T--DST--------------SRC----------------------------------------------
   95   17.4994  DCE             «DTE               HDLC C RR   NR=4        P/F=1
   96    0.0182  DTE             «DCE               HDLC R RR   NR=4        P/F=1
   97    8.4760  DTE             «DCE               HDLC C RR   NR=4        P/F=1
   98    0.0068  DCE             «DTE               HDLC R RR   NR=4        P/F=1
   99    2.4201  2156901044      «031344152574301   HDLC C I    NR=4 NS=4   P/F=0
  100    0.0181  DTE             «DCE               HDLC R RR   NR=5        P/F=0
  101    0.5892  031344152574301«2156901044         HDLC C I    NR=5 NS=4   P/F=0
  102    0.0260  2156901044      «031344152574301   HDLC C I    NR=5 NS=5   P/F=0
  103    0.0181  DTE             «DCE               HDLC R RR   NR=6        P/F=0
-------------------------------------Frame 96 of 4059--------------------------------
DETAIL
 DLC:   Source = DCE
 DLC:
 HDLC:  ----- High Level Data Link Control (HDLC) -----
 HDLC:
 HDLC:  Address = 01 (Response)
 HDLC:  Control field = 91
 HDLC:      100. .... = N(R) = 4
 HDLC:      ...1 .... = Poll/Final bit
 HDLC:      .... 0001 = RR  (Receive ready)
-------------------------------------Frame 96 of 4059--------------------------------
                           Use TAB to select windows            File: SUNX253.SYC
1       2 Set   3Expert 4 Zoom  5       6Disply 7 Prev  8 Next  9Select 10 New
  Help    mark  window    in     Menus  options  frame   frame   frame  capture
```

LAPB use of Poll / Final bit

Frame Sent with Poll bit set to 1	Response Required with Final Bit set to 1
SABM / SABME, DISC	UA, DM
I (Information Transfer)	RR, REJ, RNR, FRMR
I (Disconnected Mode)	DM
Supervisory (RR, RNR, REJ)	RR, REJ, RNR, FRMR

LAPB has a specific procedure for using the P/F bit. The station, upon receiving a SABM/SABME, DISC, Supervisory frame, or Information frame with P=1, must set the F to 1 in the next response it transmits. The following conventions in the slide apply.

Following an HDLC Session

MARY	Delta T	DST	SRC	
1		DCE.HDLC.01	«DTE.HDLC.01	HDLC 01 SABM P/F=1
2	0.0412	DTE.HDLC.01	«DCE.HDLC.01	HDLC 01 UA P/F=1
3	0.0492	DCE.HDLC.01	«DTE.HDLC.01	HDLC 01 I NR=0 NS=0 P/F=0
4	0.0408	DTE.HDLC.01	«DCE.HDLC.01	HDLC 01 RR NR=1 P/F=0
5	0.0438	DTE.HDLC.03	«DCE.HDLC.03	HDLC 03 I NR=1 NS=0 P/F=0
6	0.0287	DCE.HDLC.03	«DTE.HDLC.03	HDLC 03 RR NR=1 P/F=0
7	9.8700	DCE.HDLC.01	«DTE.HDLC.01	HDLC 01 I NR=1 NS=1 P/F=0
8	0.0379	DTE.HDLC.01	«DCE.HDLC.01	HDLC 01 RR NR=2 P/F=0
9	0.3000	DTE.HDLC.03	«DCE.HDLC.03	HDLC 03 I NR=2 NS=1 P/F=0
10	0.0288	DCE.HDLC.03	«DTE.HDLC.03	HDLC 03 RR NR=2 P/F=0
11	0.6967	DCE.HDLC.01	«DTE.HDLC.01	HDLC 01 I NR=2 NS=2 P/F=0
12	0.0379	DTE.HDLC.01	«DCE.HDLC.01	HDLC 01 RR NR=3 P/F=0
13	0.2033	DTE.HDLC.03	«DCE.HDLC.03	HDLC 03 I NR=3 NS=2 P/F=0
14	0.0288	DCE.HDLC.03	«DTE.HDLC.03	HDLC 03 RR NR=3 P/F=0
15	5.7234	DCE.HDLC.01	«DTE.HDLC.01	HDLC 01 I NR=3 NS=3 P/F=0
16	0.0413	DTE.HDLC.01	«DCE.HDLC.01	HDLC 01 RR NR=4 P/F=0
17	0.0867	DTE.HDLC.03	«DCE.HDLC.03	HDLC 03 I NR=4 NS=3 P/F=0
18	0.0288	DCE.HDLC.03	«DTE.HDLC.03	HDLC 03 RR NR=4 P/F=0
19	0.0333	DCE.HDLC.01	«DTE.HDLC.01	HDLC 01 I NR=4 NS=4 P/F=0
20	0.0413	DTE.HDLC.01	«DCE.HDLC.01	HDLC 01 RR NR=5 P/F=0

Frame 1 of 46

File: MODULO8.SYC

1 Help | 2 Set mark | 3Expert window | 5 Menus | 6Disply options | 7 Prev frame | 8 Next frame | 9Select frame | 10 New capture

SNIFFER® UNIVERSITY

HDLC 6 - 42

Internetwork Analysis and Troubleshooting, 10/96, Rev. 5.0

Network General

It's important to first benchmark a normal HDLC session establishment to use as a basis for future comparison when problems occur. Session establishment times may vary according to the link speed and processor speed of the DTE or DCE. In this trace, the link speed is only 2400 bps.

How long does it take for session establishment to complete?

Please record this time.
Frame 166 shows the first DM.
When the data transfer is complete and one side of the connection wants to terminate the link, it will send a DISC command. The other side will respond with the UA.

Following an HDLC Session Using Two-Station Format & DLC Addresses

MMARY	Delta T	From DTE	From DCE
1		HDLC 01 SABM P/F=1	
2	0.0412		HDLC 01 UA P/F=1
3	0.0492	HDLC 01 I NR=0 NS=0 P/F=0	
4	0.0408		HDLC 01 RR NR=1 P/F=0
5	0.0438		HDLC 03 I NR=1 NS=0 P/F=0
6	0.0287	HDLC 03 RR NR=1 P/F=0	
7	9.8700	HDLC 01 I NR=1 NS=1 P/F=0	
8	0.0379		HDLC 01 RR NR=2 P/F=0
9	0.3000		HDLC 03 I NR=2 NS=1 P/F=0
10	0.0288	HDLC 03 RR NR=2 P/F=0	
11	0.6967	HDLC 01 I NR=2 NS=2 P/F=0	
12	0.0379		HDLC 01 RR NR=3 P/F=0
13	0.2033		HDLC 03 I NR=3 NS=2 P/F=0
14	0.0288	HDLC 03 RR NR=3 P/F=0	
15	5.7234	HDLC 01 I NR=3 NS=3 P/F=0	
16	0.0413		HDLC 01 RR NR=4 P/F=0
17	0.0867		HDLC 03 I NR=4 NS=3 P/F=0
18	0.0288	HDLC 03 RR NR=4 P/F=0	
19	0.0333	HDLC 01 I NR=4 NS=4 P/F=0	
20	0.0413		HDLC 01 RR NR=5 P/F=0

Frame 1 of 46

Use TAB to select windows File: MODUL08.SYC

1 Help	2 Set mark	3Expert window	4 Zoom out	5 Menus	6Disply options	7 Prev frame	8 Next frame	9Select frame	10 New capture

HDLC 6 - 43

HDLC Exercise

Objective: Study the cause of HDLC FRMRs.

Background: The Network manager has noticed it sometimes takes a long time to set up an X.25 virtual circuit. This is a network of ISO traffic running over an X.25 link.

1. Load the file C:\SYCAP\TC107\SUNX253.SYC.

2. Display the Expert Overview screen. Arrow down to the DLC stations layer, highlight the **Objects/Symptoms** statistics, and press **Enter**. There are 4 FRMR (frame rejects) symptoms. Highlight the **4 FRMR frame reject** symptoms on the Data Link Station Summary screen. Press **F1 Explain**. What reason does the Explain screen give for the frame rejects?

3. Press **Esc** to return to the Data Link (DLC) Station Summary window. Go to **frame 54** to locate and display the FRMRs. Examine the **Detail** window to determine what is wrong with the Control field of the rejected frames. Why do these frames get rejected?

HDLC Exercise

Conclusion

4. What happens next?

5. Follow the session building process at the beginning of the trace. In what frame is the first session initialization frame sent?

6. In which frame is the session establishment complete at the data link layer?

7. How long does it take to establish the HDLC session?

8 How much longer before the first X.25 packet is sent?

9. What might you do to fix the long session establishment time?

Summary

- The data link layer protocol provides many services.
- HDLC uses primary, secondary and combined stations in unbalanced, symmetrical or balanced configurations.
- Normal, Asynchronous Response and Asynchronous Balanced modes are used for HDLC operations.
- HDLC uses Information, Supervisory and Unnumbered frames throughout the session.
- LAPB address fields link to a particular device.
- The SABM, UA, DISC, DM, FRMR control the flow of an HDLC session.
- The individual bits in the control field affect and indicate the operation of the connection.

Frame Relay

Objectives

On completion of this section, you will:

- Understand the differences between Frame Relay and X.25 protocols.
- Be able to identify the purpose of the fields within the address field of the frames.
- Know the congestion avoidance and recovery strategies available for Frame Relay.

Overview

- Fast packet technology that eliminates error checking at each network node.
- Well-suited for LAN applications due to support for sporadic bursts of traffic without dedicated bandwidth.
- Allows variable length frames, which cause variable delays making Frame Relay not well suited for voice and video.
- Supports Switched Virtual Circuits (SVCs) and Permanent Virtual Circuits (PVCs).
- Operates at Layer 2 of the OSI model.

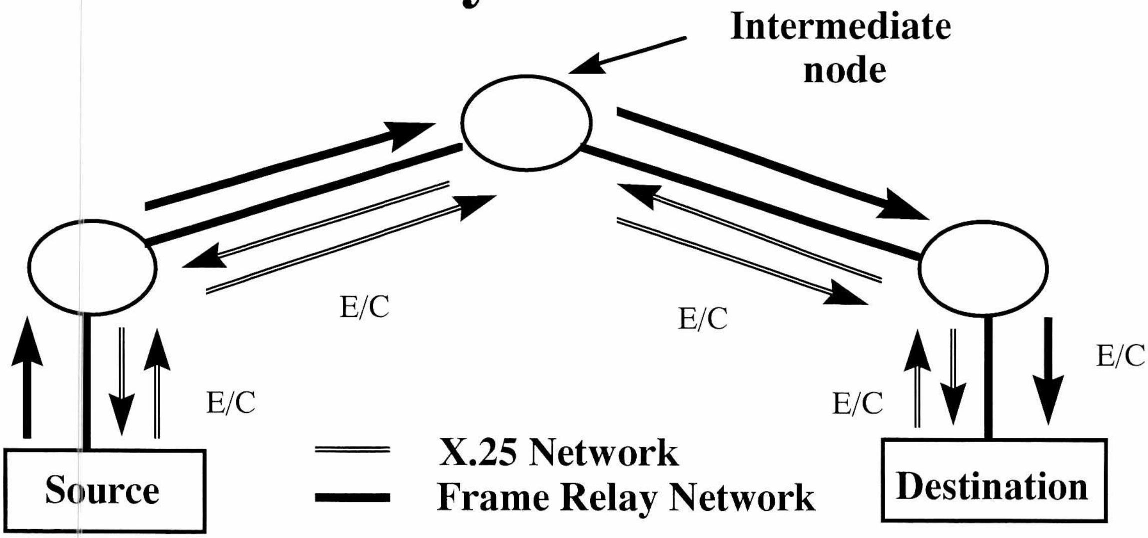
Frame Relay is a standard described under the CCITT's I-series recommendations as 1988 I.122 "Framework for additional Packet Mode Bearer Services". The term *frame-mode bearer service* (FMBS) has been used to describe services offered to the user and *Frame Relay* used to describe the protocol. Nowadays, *Frame Relay* refers to both.

Since 1988, the CCITT has come out with two interim recommendations and the ANSI has issued a standard described under ANSI T1S1/88-2242 as "Frame Relay Bearer Service."

Many Frame Relay equipment vendors support CCITT or ANSI or both. In fact, the Frame Relay Implementor's Forum was formed for the purpose of accelerating the acceptance and implementation of the Frame Relay standards. To this end, they developed an additional standard, the LMI specification.

Frame Relay frames can vary from a few bytes to well over a thousand bytes. While this feature is ideal for LANs, it makes implementation for voice or video more complex. Delay varies proportionately with the length of the frame. Voice and compressed video are intolerant of variable delays. For this reason, the ANSI committee has recommended Frame Relay for data only. Many vendors have overcame the delay issue with voice and video and offer Frame Relay as a transport for them.

One Packet Sent with Frame Relay and X.25

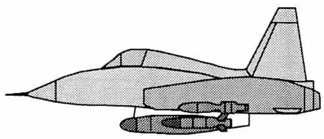
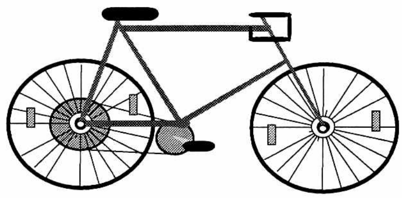


With X.25, error checking and flow control are done at each node along the way. These services are the responsibility of the upper-layer protocols of the end devices, if implemented with Frame Relay.

E/C = error check

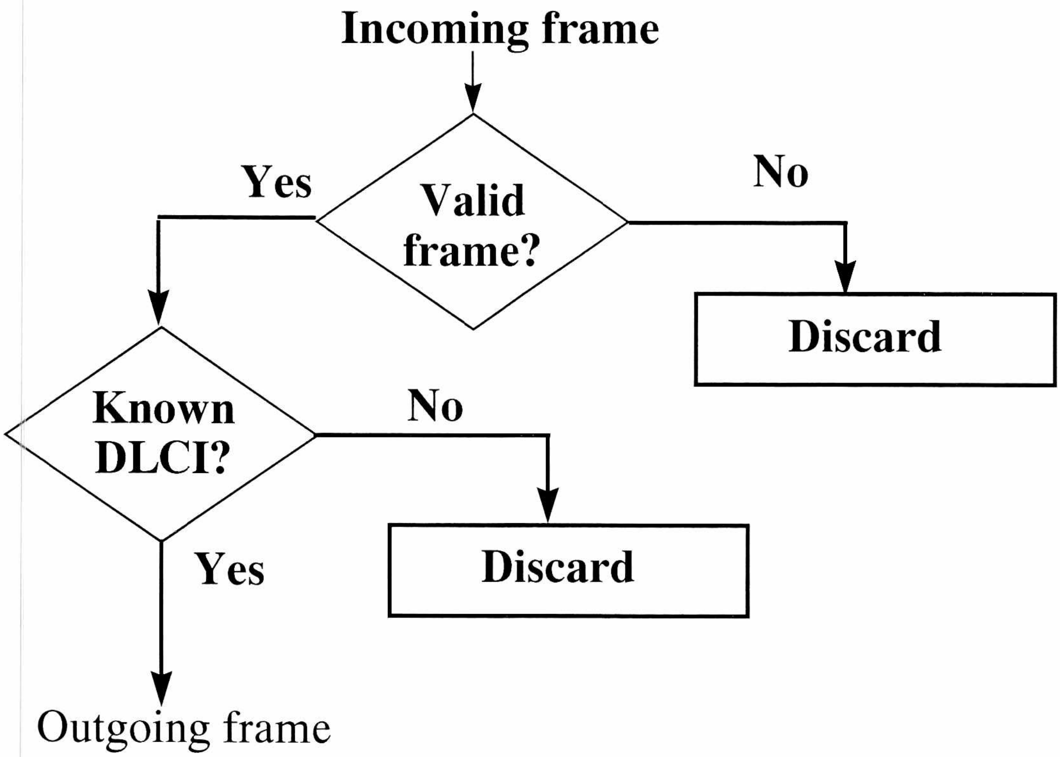
Frame relay was designed to eliminate much of the overhead associated with X.25.

Frame Relay is Faster than X.25

	Frame Relay	X.25
Session establishment	Q.931 if Frame Relay is used over the ISDN D-channel.	Well defined call-control procedure to setup and close virtual circuits.
+		
Error/flow control	Not specified; left to upper-layer protocols such as TCP to provide at end points.	Specified in protocol and accomplished at each intermediate hop.
+		
Medium	Designed for relatively noise-free digital lines including fiber.	Designed for analog noise-prone copper wire.
=		
Speed		

Currently, Frame Relay operates at 2 Mbps (E1 speeds), but has the potential to operate in the Gbps range.

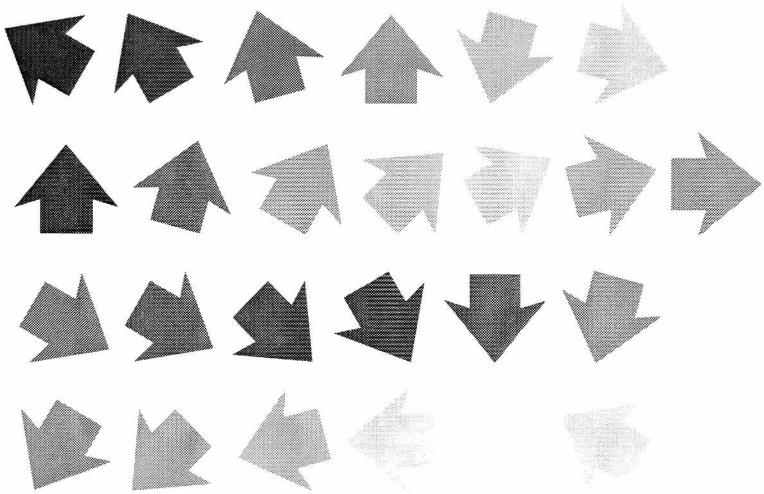
Frame Relay Call Processing



A frame is considered valid if the HDLC checksum is correct.

The DLCI is the Data Link Connection Identifier, analogous to the LCN (logical channel number) in X.25. Essentially, it's an address. The intermediate nodes merely check to see if the frame is valid and if it is a recognized DLCI. Any other condition causes the frame to be discarded. It's up to the upper-layer protocols at the end points to provide reliability.

X.25 Call Processing



Call processing for X.25 is very involved.

Protocol Stack Comparison

X.25	Network layer	
LAPB OR LAPD	Data link layer	Q.922 core
	Physical layer	

X.25 **Frame Relay**

The fact that Frame Relay operates at layer 2 of the OSI model is the main reason it is faster than X.25.

Frame relay and X.25 are not mutually exclusive protocols. Frame relay supports X.25 just as cell relay, when it is available, will support Frame Relay.

LAP-D, Link Access Protocol- D Channel is specified in CCITT Q.921. Q.922, which Frame Relay uses, is a subset of the complete LAP-D and does not implement the error recovery. LAP-D was selected as the link layer protocol for Frame Relay because virtually all upper-layer protocols, both standards based such as TCP/IP and X.25, and proprietary such as DECnet, can be run over Frame Relay.

Frame Relay Applications

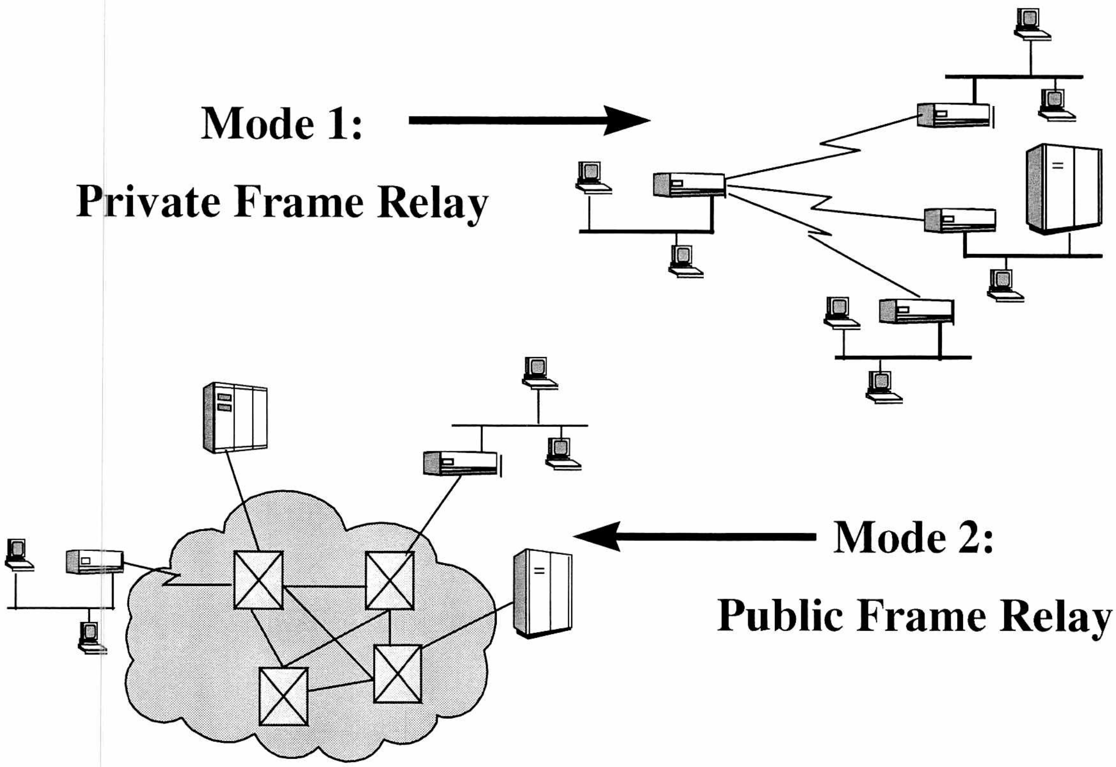
Any application requiring either low delay or high throughput. Some ANSI T1.606 suggested applications include:

- **Block-interactive:** High resolution graphics such as CAD/CAM, require low-delay and high throughput.

- **File transfer:** Large graphics file transfers require high throughput.

- **Character-interactive traffic:** Text editing and terminal emulation require low delay.

Modes of Operation



Frame Relay can be implemented either wholly by the customer, or through a public network. The difference is that through a private network, the customer controls all switching of the traffic (implementing and maintaining switch tables, etc.), whereas the provider in a public network is responsible for switching the traffic.

Frame Relay Frame Format

Flag	Address	Information		FCS	Flag
1 Byte	2-4	Variable	Length	2	1

Flag: Serves as frame delimiter. Always **01111110**. A single flag can be used as the ending flag for one frame and the beginning flag on the next.

Address: Data Link Connection Identifier (DLCI) of 10, 17, or 24 bits. Defaults to 2 bytes, may be extended to 3 or 4.

FCS: Frame-check sequence contains a 16- or 32-bit cyclic redundancy check for error control, and is performed on all fields except flags.

Frame Relay's frame format is similar to LAPB and LAPD, (both based on HDLC) with one obvious difference: no control field. As a result, there is only one frame type which is used for carrying data. As you might expect, there are no supervisory frames for providing error and flow control, and no sequence numbers.

DLCI - serves the same purpose as the Logical Channel Number (LCN) in X.25: it allows multiple logical connections to be multiplexed over a single channel. Each end of the connection assigns the unique local DLCI.

The Frame Relay specification allows for a variable length information field, ranging in size from 1 to 65,536 bytes.

Early Frame Relay Header Format

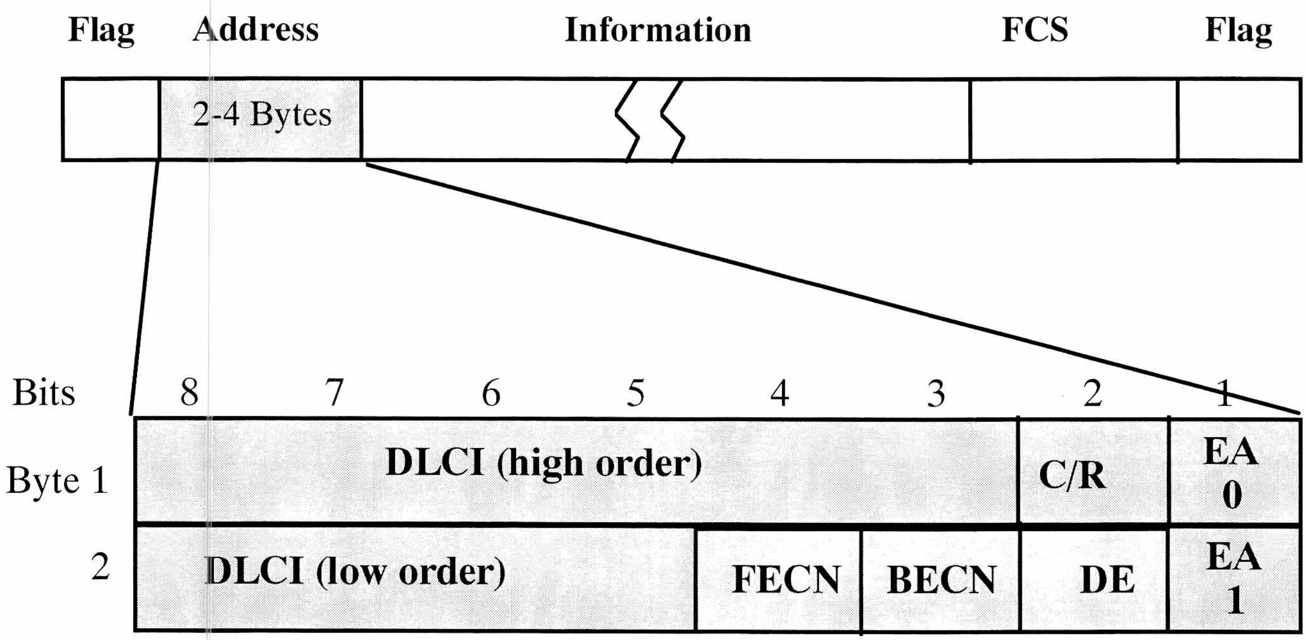
```
DETAIL
 DLC:   ----- DLC Header -----
 DLC:
 DLC:   Frame 1 arrived at  14:18:56.6157; frame size is 50 (0032 hex) bytes.
 DLC:   Destination = DTE
 DLC:   Source = DCE
 DLC:
 FRELAY: ----- Frame Relay -----
 FRELAY:
 FRELAY: Address word = 0C51
 FRELAY:  0000 11..  0101 .... = DLCI 53
 FRELAY:  .... ..0.  .... .... = Response
 FRELAY:  .... ....  .... 0... = No forward congestion
 FRELAY:  .... ....  .... .0.. = No backward congestion
 FRELAY:  .... ....  .... ..0. = Not eligible for discard
 FRELAY:  .... ....  .... ...1 = Not extended address
 FRELAY:
 ETYPE: Ethertype  = 0800 (IP)
 ETYPE:
 IP:   ----- IP Header -----
 IP:
                          Frame 1 of 420
                                               File: FSFR01-R.SYC
1      2 Set  3Expert       5       6Disply 7 Prev  8 Next  9Select 10 New
 Help   mark   window        Menus  options  frame   frame  frame   capture
```

RFC 1490 Frame Relay Header Format

```
DETAIL
FRELAY: ----- Frame Relay -----
FRELAY:
FRELAY: Address word = 0451
FRELAY:  0000 01..  0101 .... = DLCI 21
FRELAY:  .... ..0.  .... .... = Response
FRELAY:  .... ....  .... 0... = No forward congestion
FRELAY:  .... ....  .... .0.. = No backward congestion
FRELAY:  .... ....  .... ..0. = Not eligible for discard
FRELAY:  .... ....  .... ...1 = Not extended address
FRELAY:
FRELAY: ----- Multiprotocol over Frame Relay -----
FRELAY:
FRELAY: Control, pad(s) = 0300
FRELAY: NLPID = 0x80 (SNAP)
FRELAY:
SNAP: ----- SNAP Header -----
SNAP:
SNAP: Type = 0806 (ARP)
SNAP:
ARP:  ----- ARP/RARP frame -----
                              Frame 1 of 2
                         Use TAB to select windows                File: ARP.SYC
1       2 Set  3Expert 4 Zoom 5        6Disply 7 Prev  8 Next  9Select 10 New
  Help    mark  window   out    Menus  options   frame   frame   frame capture
```


Frame Relay 7 - 13

Address Field (2 Byte Default)



Demonstration file:

C:\SYCAP\TC107\FRELAY.SYC

DLCI: 10 bits long and identifies the frame's logical connection number within the multiplexed physical channel. Up to 1024 logical channels are available (2^10).

C/R: Application specific and not used by the Frame Relay protocol.

EA: Extended Address bits. Will be 0..1 for 2 byte addresses. If 3 or 4 byte DLCIs are used, these bits will be set to 0.0.

We won't discuss 3 and 4 byte addressing since they aren't widely implemented at this time.

Frame Relay Address Field

```
SUMMARY—Delta T—DST————————————SRC——————————————————————————————————————————
M    1              [164.55.2.4]    «[164.55.11.100]  RLOGIN C PORT=1020 p
     2    0.0736    [164.55.11.100]«[164.55.2.4]      TCP D=1020 S=513    ACK=1
     3    0.0017    [164.55.11.5]   «[164.55.2.4]     TCP D=1023 S=513    ACK=7
     4    0.0210    3.Intel 03F748 «1.Novell15CAAD    IPX SPX A D=0xBFC3 S=0x78D
     5    0.0601    [164.55.2.4]    «[164.55.11.100]  RLOGIN C PORT=1020 o
     6    0.0019    [164.55.2.4]    «[164.55.11.5]    RLOGIN C PORT=1023 ex
     7    0.1294    [164.55.11.100]«[164.55.2.4]      TCP D=1020 S=513    ACK=1
     8    0.0003    [164.55.11.5]   «[164.55.2.4]     TCP D=1023 S=513    ACK=7
     9    0.0845    [164.55.2.4]    «[164.55.11.100]  RLOGIN C PORT=1020 la
————————————————————————————————Frame 1 of 420——————————————————————————————
DETAIL——————————————————————————————————————————————————————————————————————
  FRELAY: ----- Frame Relay -----
  FRELAY:
  FRELAY: Address word = 0C51
  FRELAY:  0000 11..  0101 .... = DLCI 53
  FRELAY:  .... ..0.  .... .... = Response
  FRELAY:  .... ....  .... 0... = No forward congestion
  FRELAY:  .... ....  .... .0.. = No backward congestion
  FRELAY:  .... ....  .... ..0. = Not eligible for discard
  FRELAY:  .... ....  .... ...1 = Not extended address
————————————————————————————————Frame 1 of 420——————————————————————————————
                          Use TAB to select windows          File: FSFR01-R.SYC
1        2 Set   3Expert  4 Zoom  5          6Disply  7 Prev  8 Next  9Select  10 New
  Help     mark   window    in     Menus     options   frame   frame   frame   capture
```

Data Link Connection Identifiers

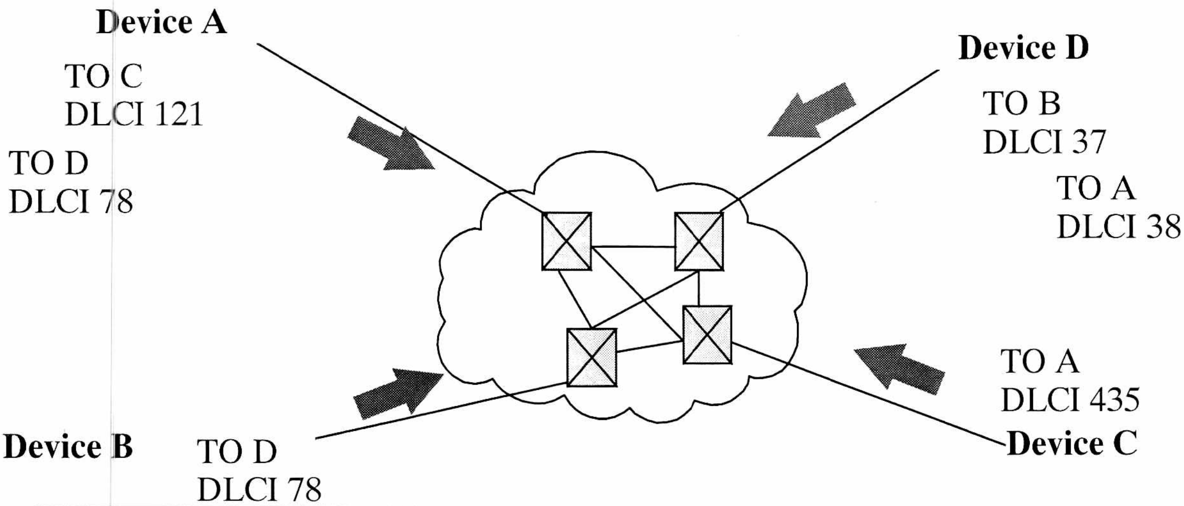
Range	Usage
0	Call Control Signaling
1-15	Reserved
16-1007	Locally assigned to carry user data
1008-1022	Reserved
1023	Local Management Interface

The above assignment of DLCIs conforms to the LMI standard. DLCI assignments specified by the ANSI and CCITT standards vary slightly. Within the frame relay protocol there are certain DLCIs that are reserved for network usage. The table above details the usage of DLCIs for a 2-octet frame relay header address field; these recommendations are based upon those detailed in the ANSI and CCITT specifications. Consequently, only 976 DLCIs are available for use by the end device at any frame relay interface. Multicast DLCI's are normally 1009-1022.

DLCI 0: Call Control Signaling

```
SUMMARY  Delta T  DST                SRC
  119             DCE.DLCI.0         «DTE.DLCI.0      LMI Keep Alive Status En
  120    0.0028   DTE.DLCI.0         «DCE.DLCI.0      LMI Keep Alive Status
  277    9.9904   DCE.DLCI.0         «DTE.DLCI.0      LMI Keep Alive Status En
  278    0.0029   DTE.DLCI.0         «DCE.DLCI.0      LMI Keep Alive Status

                              Frame 119 of 420
DETAIL
 FRELAY: ----- Frame Relay -----
 FRELAY:
 FRELAY: Address word = 0001
 FRELAY:  0000 00..  0000 .... = DLCI 0 (Signalling)
 FRELAY:  .... ..0.  .... .... = Response
 FRELAY:  .... ....  .... 0... = No forward congestion
 FRELAY:  .... ....  .... .0.. = No backward congestion
 FRELAY:  .... ....  .... ..0. = Not eligible for discard
 FRELAY:  .... ....  .... ...1 = Not extended address
                              Frame 119 of 420
                          Use TAB to select windows          File: FSFR01-R.SYC
1       2 Set   3Expert 4 Zoom  5       6Disply 7 Prev  8 Next  9Select 10 New
 Help    mark   window   in      Menus  options  frame   frame   frame  capture
```

Operation and Mapping of DLCIs



Originating device	DLCI	TO	Destination Device	DLCI
Device A	121	TO	Device C	435
Device B	78	TO	Device D	37
Device A	78	TO	Device D	38

The DLCI in the frame relay frame is used to identify the logical channel between the user and the network, and has only a local significance: it does not relate to any network-wide address. Any data frames passed over the logical circuit carry the same DLCI regardless of whether the traffic is passing from the user or to the user.

In this example, device A is communicating to device C on local DLCI 121, but at the remote end device C is using DLCI 435 to communicate with Device A.

Since the DLCIs have only local significance, it is the responsibility of the network to map the access DLCIs to the destination DLCIs. The local significance of the DLCIs also enables DLCIs to be reused at different interfaces. In this example both device A and device B use DLCI 78.

Congestion Control

Bits	8	7	6	5	4	3	2	1
Byte 1	**DLCI (high order)**						**C/R**	**EA 0**
2	**DLCI (low order)**				**FECN**	**BECN**	**DE**	**EA 1**

FECN: Forward Explicit Congestion Notification signals the receiver that the frame has encountered congestion.

BECN: Backward Explicit Congestion Notification signals the transmitter that congestion avoidance should begin.

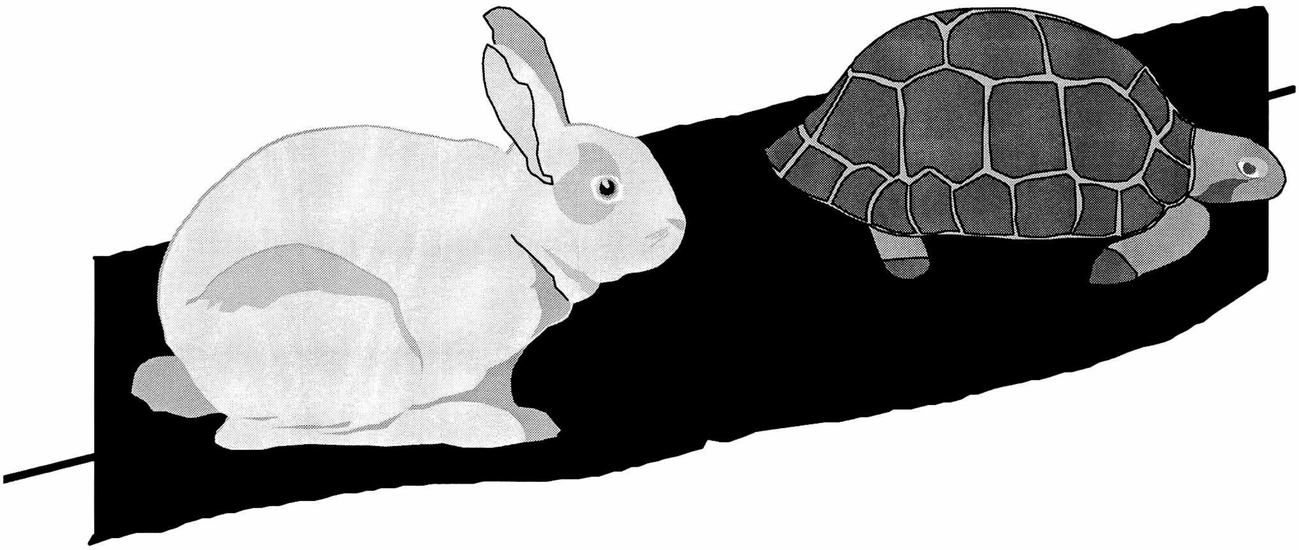
DE: Discard Eligibility bit, when set to 1, indicates this frame should be discarded in preference to other frames in which this bit is set to 0.

We will discuss the FECN, BECN, and DE bits in the next pages.

BECN & DE

```
CAPTURING     ============DLC Stats: DTE.DLCI.21================00:00:34
   Total frames:            1116        Total bytes (w/header):      716165
                                        Average frame length (bytes):   641
   Absolute utilization:    1.70%       Relative utilization:           34%

   Forward congestion:       0          Measured  bandwidth:   211008 bps
   Backward congestion:     54            (recomputed every 2 seconds)
   Discard eligibility:    260          Requested bandwidth:    64000 bps
   PVC is active

   14 network stations associated with this DLC station:
   SLEEPY                  QMC1_________________..  PRINCE-CHARMING
   QMC1_________________.. WITCH                    SNEEZY
   MMIS_APP3               994204.FFFFFFFFFFFF      HAPPY
   CINDERELLA              161.69.97.127            MMIS_APP1
   GRUMPY                  QMC1_________________..
 ==========2 of 16; Use ↑↓; +- for next/prev symptom; ESC to return==========
     0 CRC Errors    RxC  TxC  RxD  TxD  CTS  RTS  DSR  DTR      0 Lost Frames
Frames:      2056 Seen      2056 Accepted,        824 Kbytes     23% Buffer use
DTE                                     DCE
  0     6  16   60   200  1200   7000   0     6  16   60   200   1200   7000
                        Frames per second
                                                              9      10 Stop
                                                              Pause  capture
```

How Congestion Control Works...



SNIFFER® UNIVERSITY

Frame Relay 7 - 21

Internetwork Analysis and Troubleshooting, 10/96, Rev. 5.0

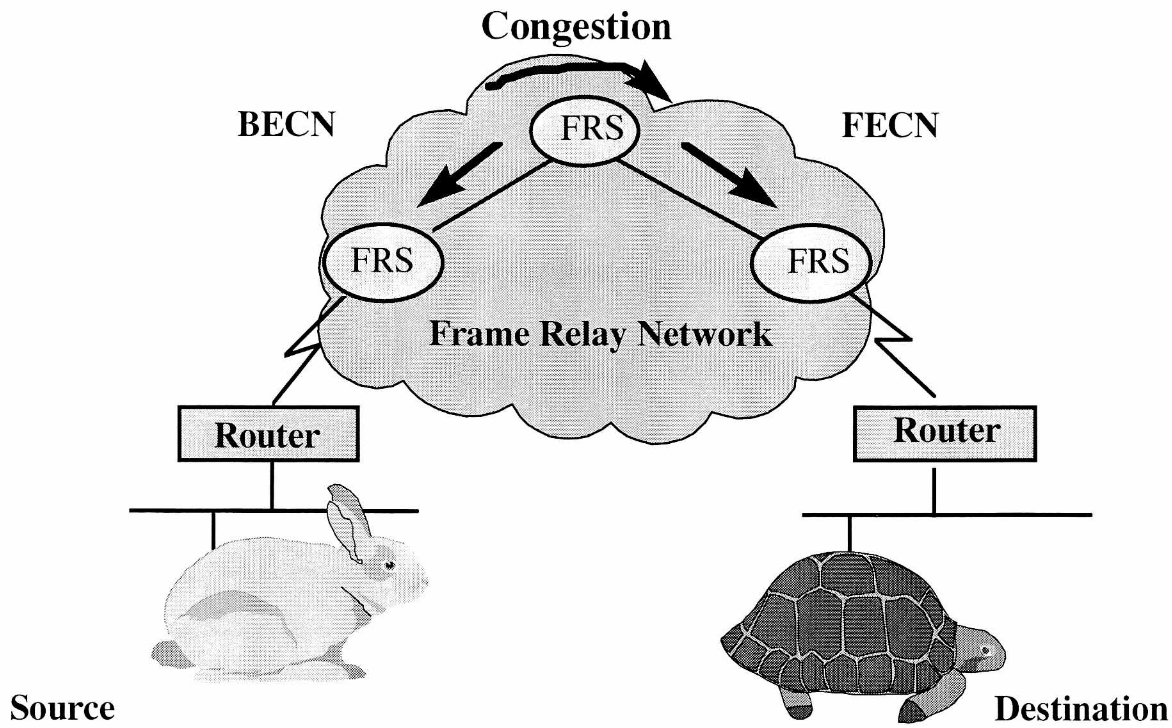
Network General

Two Congestion Control Strategies

- **Congestion-avoidance** procedures are carried out by the **network** using **explicit signaling** methods at the onset of congestion, to minimize network degradation.
- **Congestion-recovery** procedures are carried out by the **end users** using **implicit signaling** methods, to prevent the network from failing when faced with severe congestion. When end users detect dropped frames, congestion is implied. The network participates in congestion recovery by using the Discard Eligibility bit.

Congestion control is the joint responsibility of the network and the end users.

Congestion Avoidance

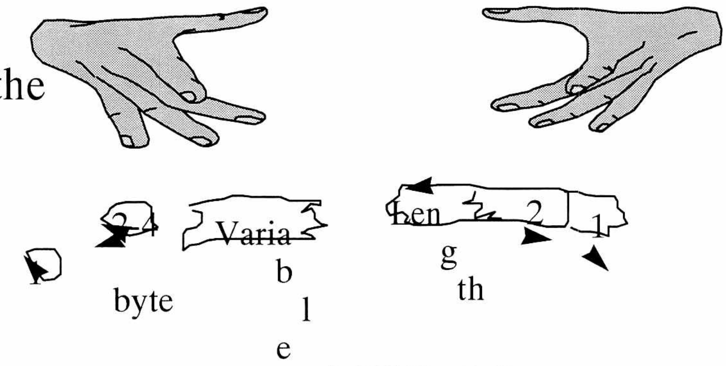


FRS = Frame relay switch. If the source received a frame with the BECN bit set, it *should* initiate congestion avoidance procedures in the opposite direction of the received BECN. The source would simply reduce the number of frames sent until the congestion cleared (no BECNs received).

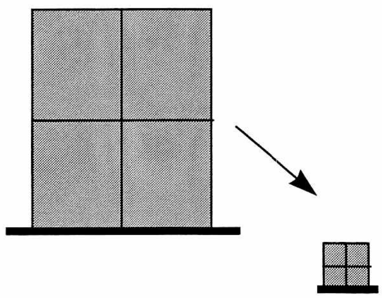
Action taken upon receiving a FECN bit is more involved, since it requires notifying the user on the other end to restrict their flow of frames. The Frame Relay standard does not specify how the end node should handle forward congestion. If the destination receives an FECN frame, indicating congestion has occurred in the same direction as the received frame, some higher layer protocol can implement flow control, and reduce the number of frames received. A higher layer protocol such as TCP or X.25 could respond by reducing the window size thus restricting the number of bytes or frames the other end could send.

End User Congestion Recovery

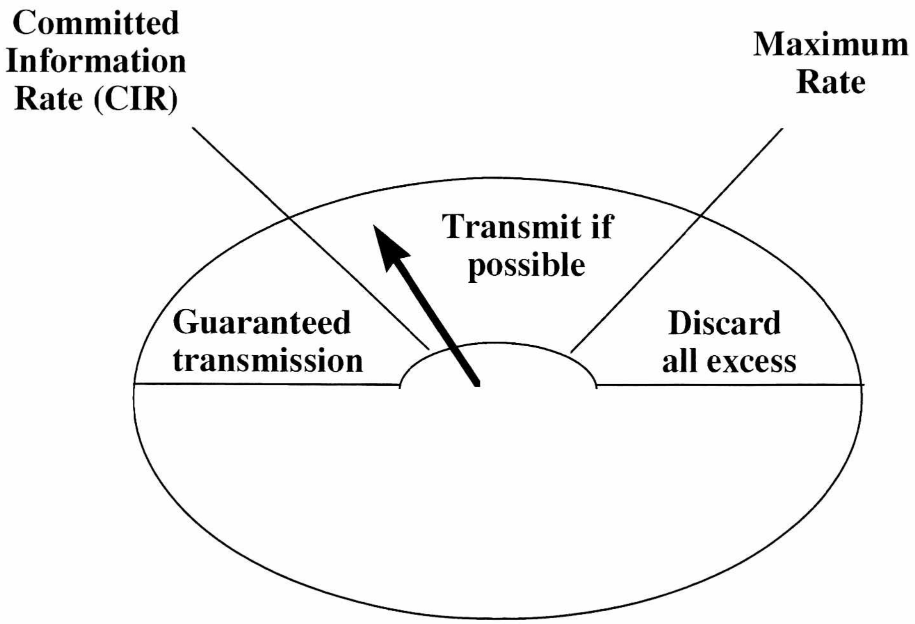
When a frame is dropped by the network...



...higher layer protocols such as TCP or SPX may deduce that congestion exists and reduce the “window size”, and restrict the number of frames or bytes the other side can send.



Network Congestion Recovery



Source: T. Jones, K. Rehbehn, and E. Jennings, *The Buyer's Guide to Frame Relay Networking* (Herndon, VA.: Netrix Corporation, 1991).

Each user can negotiate a *committed information rate* (CIR) in bps at setup time which is an estimate of its generated load during busy periods. The network responds with a guaranteed CIR in the absence of errors which may be less than or equal to the requested CIR. The frame handler, to which the user is attached, meters the user's traffic, and will not alter the DE (discard eligibility) bit, if the transmission rate is less than the guaranteed rate. The frame handler will set the DE bit on frames above the CIR, but less than the maximum, but will still **forward** the frame. These frames may reach their destination or may get discarded by a Frame Relay switch if congestion occurs. Finally, a *maximum information rate* is set and all frames beyond that are discarded.

CIR Exceeded

```
SUMMARY—Delta T—DST——————————————SRC——————————————————————————————————————
M    1           994204.FFFFFF..«994204.W11f1t..  IPX RIP response: 36 netwo
     2   0.0022  994204.FFFFFF..«994204.W11f1t..  IPX RIP response: 36 netwo
     3   0.0022  994204.FFFFFF..«994204.W11f1t..  IPX RIP response: 36 netwo
     4   0.0022  994204.FFFFFF..«994204.W11f1t..  IPX RIP response: 36 netwo
═══════════════════════Data Link (DLC) Station Summary═══════════════════════
 DLC Station        FrmsSent  FrmsRcvd  Symps  Last Symptom
 DCE                    4770      6787      0
 DTE.DLCI.1023            22        22      0
 DTE.DLCI.16             524       358      0
 DTE.DLCI.17             467       295      0
 DTE.DLCI.18             880       715      1  CIR exceeded (64064 bps)
 DTE.DLCI.19             191        19      5  CIR exceeded (54336 bps)
 DTE.DLCI.20             717       433      0
 DTE.DLCI.21            2538      2722     45  CIR exceeded (124768 bps)
 DTE.DLCI.22             185        26      0
 DTE.DLCI.23             175        17     30  CIR exceeded (6272 bps)
 DTE.DLCI.24             175        11      0
 DTE.DLCI.26             175        11      5  CIR exceeded (54336 bps)
 DTE.DLCI.27             175        25      3  CIR exceeded (54336 bps)
 DTE.DLCI.28             175        25      5  CIR exceeded (54336 bps)
═══1 of 16; Use ↑↓, ENTER for detail; +- for next/prev symp; ESC to return═══
    Use F2 to filter frames on this DLC station and return to data display
1       2Filter 3 Data  4 View  5       6Disply         8Higher         10 New
Explain &disply display  bytes  Menus   options          layer          capture
```

Consolidated Link Layer Management

- ANSI has provided Consolidated Link Layer Management (CLLM) as an alternative to BECN/FECN congestion control method. CLLM is optional and may be used instead of or in addition to BECN/FECN.
- The Frame Relay standard does not allow the network to generate its own frames on the congested DLCI circuit. Setting the BECN and FECN will only work if a frame happens to be going in the backward or forward direction at congestion time.
- If CLLM is implemented, DLCI 1023 is reserved for sending management and control messages from the network to the Frame Relay interface.
- Each one-byte CLLM message contains: the cause of congestion (excessive traffic, equipment failure, maintenance, or unknown); the duration (short term or long term); and the DLCIs that should take action to reduce their transmission rate to the CIR.

SNIFFER® UNIVERSITY

Frame Relay 7 - 27

Internetwork Analysis and Troubleshooting, 10/96, Rev. 5.0

Network General

CLLM is extremely rare, if ever used.

Local Management Interface

- Local Management Interface (LMI) is a management specification developed by Cisco, DEC, Stratacom, and Northern Telecom, and adopted by ANSI.
- The LMI, which operates between the network and the endpoints, supports:
  - Real-time status monitoring of the link.
  - "Keep-alives" between the network and CPE.
  - Notification to the user device of the minimum guaranteed bandwidth per virtual circuit.

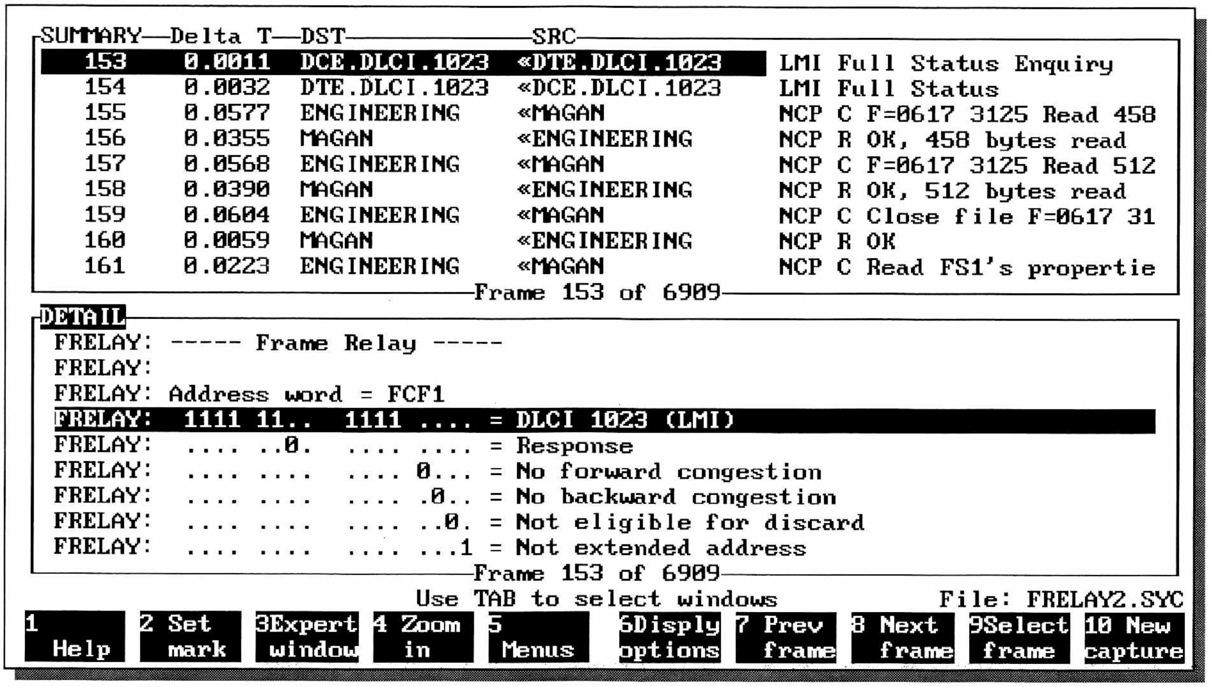
Both LMI and CLLM reserve DLCI 1023. Therefore, a given Frame Relay interface can support one or the other management scheme, but not both.

Demonstration file: C:\SYCAP\TC107\FRELAY.SYC

LMI is the most widely used of the three Frame Relay specifications:

- **LMI** utilizes DLCI 1023 and can send a change in status for multiple PVC's in 1 asynchronous update frame.
- **Annex A** utilizes DLCI 0 and needs a separate frame for each PVC when it sends update frames. It is CCITT's Q.933.
- **Annex D** also utilizes DLCI 0 and needs a separate frame for each PVC's update. It is ANSI's T1.617.

DLCI 1023


SUMMARY—Delta T—DST—SRC
153 0.0011 DCE.DLCI.1023 «DTE.DLCI.1023 LMI Full Status Enquiry
154 0.0032 DTE.DLCI.1023 «DCE.DLCI.1023 LMI Full Status
155 0.0577 ENGINEERING «MAGAN NCP C F=0617 3125 Read 458
156 0.0355 MAGAN «ENGINEERING NCP R OK, 458 bytes read
157 0.0568 ENGINEERING «MAGAN NCP C F=0617 3125 Read 512
158 0.0390 MAGAN «ENGINEERING NCP R OK, 512 bytes read
159 0.0604 ENGINEERING «MAGAN NCP C Close file F=0617 31
160 0.0059 MAGAN «ENGINEERING NCP R OK
161 0.0223 ENGINEERING «MAGAN NCP C Read FS1's propertie
Frame 153 of 6909
DETAIL
FRELAY: ----- Frame Relay -----
FRELAY:
FRELAY: Address word = FCF1
FRELAY: 1111 11.. 1111 .... = DLCI 1023 (LMI)
FRELAY: .... ..0. .... = Response
FRELAY: .... 0... = No forward congestion
FRELAY: .... .0.. = No backward congestion
FRELAY: ....0. = Not eligible for discard
FRELAY: ....1 = Not extended address
Frame 153 of 6909
Use TAB to select windows
File: FRELAY2.SYC
1 Help
2 Set mark
3Expert window
4 Zoom in
5 Menus
6Disply options
7 Prev frame
8 Next frame
9Select frame
10 New capture

LMI Message Types

- **Status Enquiry** - sent from the router (DTE) to the network switch (DCE) on a set interval.
- **Status** - sent from the network switch (DCE) to the router (DTE) in response to a Status Enquiry.

  Report types:
  - Keep Alive - reports sequence number exchange.
  - Full Status - reports sequence number exchange, multicast status, and PVC status.
- **Status Update** - sent independently from the DCE to the DTE. Reports PVC status only.

LMI Full Status

```
DETAIL
LMI:    ----- Local Management Interface -----
LMI:
LMI:    Unnumbered Information
LMI:    Local Management Interface (LMI)
LMI:    Call reference
LMI:    Message type = 7D (Status)
LMI:
LMI:    Information element 01 (Report type)
LMI:       Report type 00 (Full status message)
LMI:
LMI:    Information element 03 (Keep alive)
LMI:       Current sequence number       = 15
LMI:       Last received sequence number = 22
LMI:
LMI:    Information element 05 (Multicast status)
LMI:       Multicast group ID = 3
LMI:       Multicast DLCI     = 1019
LMI:       Source DLCI        = 101
LMI:       Multicast status = X2
LMI:              .... 00.. = Channel is present
                           Frame 4218 of 6909
                     Use TAB to select windows              File: FRELAY2.SYC
1        2 Set    3Expert  4 Zoom   5         6Disply  7 Prev   8 Next   9Select  10 New
  Help     mark   window     out      Menus   options    frame    frame    frame   capture
```

LMI Keep Alive Status

```
SUMMARY—Delta T—DST——————————————SRC————————————————————————————————————————
   153           DCE.DLCI.1023  «DTE.DLCI.1023   LMI Full Status Enquiry
   154   0.0032  DTE.DLCI.1023  «DCE.DLCI.1023   LMI Full Status
   395   9.9701  DCE.DLCI.1023  «DTE.DLCI.1023   LMI Keep Alive Status Enqu
   396   0.0020  DTE.DLCI.1023  «DCE.DLCI.1023   LMI Keep Alive Status
   701   9.9968  DCE.DLCI.1023  «DTE.DLCI.1023   LMI Full Status Enquiry
   703   0.0056  DTE.DLCI.1023  «DCE.DLCI.1023   LMI Full Status
   918   9.9932  DCE.DLCI.1023  «DTE.DLCI.1023   LMI Keep Alive Status Enqu
   919   0.0020  DTE.DLCI.1023  «DCE.DLCI.1023   LMI Keep Alive Status
  1171  10.0301  DCE.DLCI.1023  «DTE.DLCI.1023   LMI Full Status Enquiry
——————————————————————————————Frame 395 of 6909———————————————————————————————
DETAIL
 LMI:    Call reference
 LMI:    Message type = 75 (Status Enquiry)
 LMI:
 LMI:    Information element 01 (Report type)
 LMI:       Report type 01 (Sequence number exchange only)
 LMI:
 LMI:    Information element 03 (Keep alive)
 LMI:       Current sequence number       = 9
 LMI:       Last received sequence number = 1
——————————————————————————————Frame 395 of 6909———————————————————————————————
                              Use TAB to select windows        File: FRELAY2.SYC
1        2 Set   3Expert 4 Zoom  5        6Disply 7 Prev  8 Next  9Select 10 New
  Help     mark  window    in      Menus  options   frame   frame   frame capture
```


Frame Relay 7 - 32

Frame Relay Exercise 1

Objective: Become familiar with displaying Frame Relay statistics on the Sniffer Network Analyzer as an aid to verifying and troubleshooting a Frame Relay link.

Background: LAN data frames are encapsulated within Frame Relay. Multiple DLCIs are in use. LMI is active.

1. Set the **Display** protocol filter to **Frame Relay LMI** only.
2. Set **Summary** and **Detail** windows **on**, and **Expert off**.
3. Set Options/Frame Type to **Frame Relay**.
4. Set Capture to **Classic** mode.
5. Set Screen Format to: 1) **Show frame counts**
   2) **Log bar scale**
   3) **Counts**

Frame Relay Exercise 1

Continued

6. **Capture** from the trace file C:\SYCAP\TC107**FRELAY2.SYC**. Press **F10** to Capture. Hint: Holding down the **Alt** key speeds up the capture. Using the **Classic** Capture screen, answer the following:

7. How many total frames are there in this trace?
   How many LMI frames are there?

8. How many active DLCIs are there in this file?
   What are they?

9. Are the FECN, BECN, or DE bits set in any of the frames?

10. How many LMI status enquiries are there? Is the source DTE or DCE?
    How many LMI status replies are there? Is the source DTE or DCE?

Frame Relay Exercise 1

Continued

11. Press **F3** to Display Data. (Remember that the LMI filter is set.)

12. Turn on **Relative time**. By looking at the **Summary** screen, how often does the DTE issue an LMI Keep Alive Status Enquiry?

    How often for a Full Status Enquiry?

13. Are these enquiries always answered?

14. Save setup to Files/Save/Setups as **LMI**.

Frame Relay Exercise 2

Objective: To analyze LMI frames in detail on the Sniffer Network Analyzer as an aid to verifying and troubleshooting a Frame Relay link.

Background: LAN data frames are encapsulated within Frame Relay. Multiple DLCIs are in use. LMI is active.

1. **Load** the setup file C:\SYCAP\TC107**LMI.SYS**.

2. **Capture** from the trace file C:\SYCAP\TC107**FRELAY2.SYC**. Press **F10** to Capture. Hint: Holding down the **Alt** key speeds up the capture.

3. Press **F3** for Display and **Tab** into the Detail screen. Go to **frame 153**. What is the message type (decoded)?

   What is the current sequence number?

   What is the last received sequence number?

Frame Relay Exercise 2

Continued

4. Press **F8** to go to **frame 154**. What is the current sequence number?
   What is the last received sequence number?
   Is this consistent with **frame 153**?

5. What is the message type for **frame 154** (decoded)?
   Look at **Info. element 07** (PVC status). What is the bandwidth indicated?

6. Look at **Info. element 05** (Multicast status). Is a multicast DLCI indicated?
   What is the DLCI number?

7. Press **F6** for Display options. Remove the protocol filter for **Frame Relay LMI**.

Frame Relay Exercise 2

Continued

8. Turn off the **Summary** window. Turn on the **Detail** and **Hex** windows. Go to **frame 647**. Using the pattern in frame 647, build a binary pattern match display filter for multicast DLCI **1019**.

   Hint: [111111XX1011XXX...], [Offset:0].

9. Turn on the **Summary** window. Looking at the Summary screen of frames using DLCI 1019, what protocols are using this multicast DLCI?

   What type of destination addresses are shown?

10. Is this a proper use of a multicast DLCI (DLCI 1019)?

Frame Relay Exercise 3

Objective: To recognize opportunities for network optimization.

Background: The trace file used is from the earlier Protocol Forcing exercise. It involves a Frame Relay device that forwards both bridged and routed Ethernet LAN traffic over the Frame Relay network.

1. **Load** and **Display** the trace file C:\SYCAP\TC107\FSFR01.SYC. Press **F3** twice to display the data.

2. Reload the setup file, FSFR01, that we used in the Protocol Forcing exercise on the first day of class. (From the Main Menu, the keystrokes are **Files**, **Load**, **Setup**, **Enter**, **FSFR01.SYS**, **Enter**, **F3**.)

3. Now that we have finished the Protocol Force, we can examine the data. Go to frame 254. Do the Frame Relay LMI management frames appear to be sequencing properly?

Frame Relay Exercise 3

Continued

4. Examine the NetWare SAP data in frames 2 to 27, 374 to 399, etc. Is it unique data in each frame detailing the various NetWare services or is it something else? (Note that each IPX router accumulates the NetWare SAPs it receives on all ports, and sends the consolidated information out all other ports, in as few frames as possible.) Is this router propagating the Novell NetWare SAPs properly?

5. Examine the AppleTalk NBPs and their Delta times in frame 37 to 50. Does the retry interval of 0.4mS seem appropriate? Do the same for the frames 80 to 92, 117 to 129, etc.

6. The Novell NetWare IPX RIPs in frames 461 to 473 are similar to the earlier SAPs except that routes are advertised instead of services. Examine the RIP data. There should be only one IPX RIP if there is only one network route to be advertised. Also, the IPX RIPs are propagated once every 60 seconds.

Frame Relay Exercise 3

Continued

7. After looking at the excessive SAPs, IPX RIPs, IP RIPs, and NBP advertisements, does it appear as though the router has broadcasting problems?

8. Now go back and look at the SAP frames numbered 2 to 27. Examine the Ethertype/Length field within the Ethernet header of the first 13 SAPs and then the next 13 SAPs. Which frame types are being used?

9. Once again, go back and look at the SAP frames. This time examine the DLCI field within the Frame Relay header. Are all the Ethernet frames sending to the same DLCI? Are all the 802.3 frames sending to the same DLCI?

10. What changes would you make to the router configuration to minimize the number of broadcasts transmitted by the Ethernet/Frame Relay router?

Summary

- Frame Relay is faster than X.25 protocols since it operates at layer 2 of the OSI model. It uses Q.922 at the data link layer and relies on upper-layer protocols to implement error recovery procedures.
- The address field of the frames identifies the logical connection number within the physical channel and includes bits that control channel congestion.
- The network uses collision avoidance procedures using explicit signaling, while the user can use congestion-recovery procedures using implicit signaling procedures.

Point-to-Point Protocol (PPP)

Objectives

On completion of this module you should know:

- The PPP frame format and the values of common network layer protocols.
- The purpose of the three types of LCP packets.

Point-to-Point Protocol

- Proposed Internet standard specified in RFC 1331.
- Defines standard encapsulation scheme for the transport of different Network Layer protocols including but not limited to IP.
- Works over synchronous, asynchronous, dial-up, or dedicated lines.
- No restrictions on type of signaling employed or line speed.

PPP is used for sync and async leased lines but the SIA only decodes synchronous PPP.

PPP Protocol Stack

Higher layers		
Network layer	**Network-Layer Protocols** (IP, DECnet, OSI, IPX)	**Network Control Protocol** (Network-layer protocol specific)
Data link layer	**Link-Control Protocol**	
	HDLC	
Physical layer	**RS-232, RS-449, EIA-530, V.24, and V.35**	

EIA-530 is RS- 422 using a DB-25 connector.

Link Control Protocol (LCP) packets define procedures for host authentication, link maintenance, and encapsulation format negotiation.

The Network Control Protocol (another NCP acronym) manages the particular Network-Layer Protocol.

PPP Frame Format

1 Octet	1	1	2	≤ 1500	Usually 1	1
Flag	Address	Control	Protocol	Information	FCS	Flag
01111110	11111111	00000011				

Address: All-ones (FF hex) specifies the HDLC all-stations address. PPP does not use individual addresses.

Control: PPP only uses HDLC Unnumbered Information frames (03 hex).

Protocol: Specific to PPP; used to identify the upper-layer protocol, encapsulated in the Information field. In pure HDLC, this is the Extended Address field.

Demonstration file:
C:\SYCAP\TC107\PUREPPP.SYC

The SIA distinguishes PPP on the basis of the address and control bytes. Just above the DLC address, notice the ROUTER Header=FF03. The Sniffer decodes the address and control bytes and labels it the PPP Router/Bridge header.

PPP Frame Format

Continued

```
DETAIL
ROUTER: ----- PPP Router/Bridge -----
ROUTER:
ROUTER: Header = FF03
ROUTER:
PPP:   ----- Point-to-Point Protocol -----
PPP:
PPP:   Protocol = C021 (Link Control)
PPP:   Code = 01 (Configure Request)
PPP:   Identifier = 0
                                  Frame 1 of 669
HEX                                                               ASCII
0000  FF 03 C0 21 01 00 00 0A  05 06 02 17 92 33          ..@!........3

                                  Frame 1 of 669
                           Use TAB to select windows          File: PPPTELNT.SYC
1      2 Set  3Expert 4 Zoom 5       6Disply 7 Prev 8 Next 9Select 10 New
 Help   mark  window   in    Menus  options  frame  frame  frame  capture
```

Protocol Type Fields

Value Range	Value	Protocol
0-3 Network Layer protocols	0021	IP
	0023	OSI
	0027	DECNet Phase IV
	0029	AppleTalk
	002B	Novell IPX
	0035	Banyan Vines
8-B Network Control Protocols	8021	Internet Protocol Control Protocol
	8023	OSI Network Layer Control Protocol
	8027	DECNet Phase IV Control Protocol
	8029	AppleTalk Control Protocol
	802B	Novell IPX Control Protocol
C-F Link Control Protocol	C021	Link Control Protocol
	C023	Password Authentication Protocol
	C025	Link Quality Report

For a complete list, please refer to RFC 1331 available through the NIC.

Link- and IP-Control Protocol Frame Format
(1st 4 Bytes of Information Field)

1 Octet	1	2
Code	Identifier	Length

Code: Used in LCP packets to identify packet type.
Identifier: Chosen at random, used to match requests and replies.
Length: Specifies the length of the LCP packet in bytes.

Demonstration file:
C:\SYCAP\TC107\PUREPPP.SYC.
Frames 1-4 are LCP configuration packets and frames 5-7 are IPCP configuration packets.

Link Control Protocol (LCP) packets define procedures for host authentication, link maintenance, and encapsulation format negotiation.

The Internet authorities use a variation of LCP called the IP Control Protocol (IPCP). Once LCP is finished negotiating, IPCP can negotiate at the network layer. The frame format is identical to LCP.

LCP Frame Format

Continued

```
DETAIL
  PPP:   ----- Point-to-Point Protocol -----
  PPP:
  PPP:   Protocol = C021 (Link Control)
  PPP:   Code = 01 (Configure Request)
  PPP:   Identifier = 0
  PPP:   Length = 10 bytes
  PPP:   Option type = 5 (Magic number)
  PPP:   Length = 6 bytes
  PPP:   Magic number = 02179233
                                          Frame 1 of 669
HEX                                                                        ASCII
  0000   FF 03 C0 21 01 00 00 0A  05 06 02 17 92 33          △.└!.........3

                                          Frame 1 of 669
                                    Use TAB to select windows        File: PPPTELNT.SYC
1       2 Set   3Expert 4 Zoom  5       6Disply 7 Prev  8 Next  9Select 10 New
 Help    mark   window   in     Menus   options  frame   frame   frame  capture
```

Three LCP Packet Types

- **Link Configuration** - used to establish and configure a PPP link.
- **Link Termination -** used to terminate a link.
- **Link Maintenance -** used to manage and troubleshoot a link.

Link Configuration Packet Types

- **Configure Request** - sent by a host wishing to open an LCP connection. May include options for negotiating maximum packet size, type of authentication, compression type, and others.

- **Configure Ack** - positive reply to a Configure Request.

- **Configure Nak** - indicates receipt of Configure Request but one or more Configuration Options are unacceptable. Unacceptable and acceptable options will be listed in packet.

- **Configure Reject** - indicates one or more of the Configuration Options were not recognized or not accepted and negotiation is not a possibility. Options rejected will be listed in the packet. Original station should send a new packet without any of the rejected options.

Demonstration file:
C:\SYCAP\TC107\PUREPPP.SYC.
Frame 1 is a Configure Request and frame 2 is a Configure Ack.

LCP Configure Request

```
SUMMARY—Delta T—DST——————————————SRC————————————
M     1          DCE              «DTE             PPP LCP Configure Request
      2   3.0020 DCE              «DTE             PPP LCP Configure Request
      3   3.0028 DCE              «DTE             PPP LCP Configure Request
      4   3.0028 DCE              «DTE             PPP LCP Configure Request
      5   3.0024 DCE              «DTE             PPP LCP Configure Request
      6   1.3484 DTE              «DCE             PPP LCP Configure Request
      7   0.0072 DTE              «DCE             PPP LCP Configure Ack
      8   0.0012 DCE              «DTE             PPP LCP Configure Ack
      9   0.0051 DCE              «DTE             PPP IPCP Configure Request
————————————————————————————————Frame 1 of 669————————————————————
DETAIL
 PPP:  Protocol = C021 (Link Control)
 PPP:  Code = 01 (Configure Request)
 PPP:  Identifier = 0
 PPP:  Length = 10 bytes
 PPP:  Option type = 5 (Magic number)
 PPP:  Length = 6 bytes
 PPP:  Magic number = 02179233
 PPP:

————————————————————————————————Frame 1 of 669————————————————————
                            Use TAB to select windows          File: PPPTELNT.SYC
1       2 Set  3Expert 4 Zoom  5       6Disply 7 Prev  8 Next  9Select 10 New
  Help    mark  window   in      Menus options  frame   frame   frame  capture
```

Link Termination Packet Types

- **Terminate Request** - sent by the host wishing to close the session.

- **Terminate Ack** - response to Terminate Request.

Demonstration file:

C:\SYCAP\TC107\PUREPPP.SYC

Frames 7 and 8 show the Terminate Request command and the Terminate Ack response.

Link Maintenance Packet Types

- **Code Reject** - sent by any host receiving a packet with an unknown Code-field value. A copy of the rejected packet will be returned in the information frame.
- **Protocol Reject** - sent by any host receiving a packet with an unknown Protocol-field value. A copy will be returned.
- **Echo Request and Reply** - used for testing link quality and determining loopback status. During initial LCP configuration, each host randomly chooses a "Magic Number." As long as the Magic Number in an incoming packet is different from the station's own, the station can be assured the link is not in a loopback status, and is operating properly.
- **Discard Request** - may be used in as an aid in troubleshooting or testing the link. The receiver just discards the packet.

Demonstration file:
C:\SYCAPTC107\DEMOPPP.SYC
In frames 17 and 18, this trace shows the Echo Request and Reply packets with the "Magic Number."

LCP Echo Request

```
SUMMARY  Delta T  DST             SRC
   10    0.0018   DTE             «DCE             PPP IPCP Configure Request
   11    0.0047   DTE             «DCE             PPP IPCP Configure Ack
   12    0.0012   DCE             «DTE             PPP IPCP Configure Ack
   13    3.6023   DCE             «DTE             PPP LCP Echo Request
   14    0.0188   DTE             «DCE             PPP LCP Echo Reply
   15    0.3397   DTE             «DCE             PPP LCP Echo Request
   16    0.0183   DCE             «DTE             PPP LCP Echo Reply
   17    1.0505   [134.22.100..«[134.22.100..      Zeros broadcast address
                                                   RIP R Routing entries=3
                                 Frame 13 of 669
DETAIL
 PPP:  ----- Point-to-Point Protocol -----
 PPP:
 PPP:  Protocol = C021 (Link Control)
 PPP:  Code = 09 (Echo Request)
 PPP:  Identifier = 6
 PPP:  Length = 34 bytes
 PPP:  Magic number = 02179233
 PPP:  Data = 544849532049532041204D41494E54454E414E4345204543484F
 PPP:
                                 Frame 13 of 669
                          Use TAB to select windows          File: PPPTELNT.SYC
1       2 Set   3Expert 4 Zoom  5        6Disply 7 Prev  8 Next  9Select 10 New
  Help    mark  window    in      Menus  options  frame   frame   frame  capture
```

LCP Echo Reply

```
SUMMARY  Delta T  DST         SRC
     7   0.0072   DTE         «DCE        PPP LCP Configure Ack
     8   0.0012   DCE         «DTE        PPP LCP Configure Ack
     9   0.0051   DCE         «DTE        PPP IPCP Configure Request
    10   0.0018   DTE         «DCE        PPP IPCP Configure Request
    11   0.0047   DTE         «DCE        PPP IPCP Configure Ack
    12   0.0012   DCE         «DTE        PPP IPCP Configure Ack
    13   3.6023   DCE         «DTE        PPP LCP Echo Request
    14   0.0188   DTE         «DCE        PPP LCP Echo Reply
    15   0.3397   DTE         «DCE        PPP LCP Echo Request
                          Frame 14 of 669
DETAIL
  PPP:  ----- Point-to-Point Protocol -----
  PPP:
  PPP:  Protocol = C021 (Link Control)
  PPP:  Code = 0A (Echo Reply)
  PPP:  Identifier = 6
  PPP:  Length = 34 bytes
  PPP:  Magic number = 021795CD
  PPP:  Data = 544849532049532041204D41494E54454E414E43452045434484F
  PPP:
                          Frame 14 of 669
                    Use TAB to select windows           File: PPPTELNT.SYC
1      2 Set  3Expert 4 Zoom 5      6Disply 7 Prev 8 Next 9Select 10 New
 Help   mark  window   in    Menus  options  frame  frame  frame  capture
```


PPP 8 - 16

Multipoint PPP Frame Format

Flag	Address	Control	Protocol		B	E	R	R	Sequence Numbers	Info	FCS	Flag
			PID (H)	PID (L)								
	0xff	0x03	0x00	0x3d								

Address: All-ones (FF hex) specifies the HDLC all-stations address. PPP does not use individual addresses.

Control: PPP only uses HDLC Unnumbered Information frames (03 hex).

Protocol: In PPP Multilink fragments are encapsulated using the protocol identifier 0x00 - 0x3d.

(B)eginning: The beginning bit is a one bit field set to 1 on the first fragment derived from a PPP packet and is set to 0 for all other fragments from the same PPP packet.

(E)nding: The ending bit is a one bit field set to 1 on the last fragment and set to 0 for all other fragments.

A fragment may have both the beginning and ending bits set to 1.

The goal of multilink operation is to coordinate multiple independent links between a fixed pair of systems, providing a virtual link with greater bandwidth than any of the constituent members. The aggregate link, or bundle, is named by the pair of identifiers for the two systems connected by multiple links. A system identifier may include information provided by PPP authentication and information provided by LCP negotiation. The bundled links can be different physical links, as in multiple async lines, but may also be instances of multiplexed links, such as ISDN, X.25, or Frame Relay.

Multipoint PPP Frame Format

Continued

Flag	Address	Control	Protocol: PID (H)	Protocol: PID (L)	B	E	R	R	Sequence Numbers	Info	FCS	Flag
	0xff	0x03	0x00	0x3d								

(R)eserved: Reserved field whose use is not currently defined, which must be set to 0. It is 2 bits long when using short sequence numbers, 6 bits with long sequencing.

Sequence Numbers: The sequence field is a 24 or 12 bit number that is incremented for every fragment transmitted. By default, the sequence field is 24 bits long, but can be negotiated to be only 12 bits by using an LCP configuration option.

FCS: The frame check sequence is the same as in regular PPP.

There are two frame formats used in multilink PPP: long and short.

In the long frame format there is a 24 bit sequence number field with the reserved bit field being 6 bits in length.

In the short frame format there is a 12 bit sequence number field with the reserved bit field being 2 bits in length.

The short frame format for multilink PPP is shown above.

PPP Negotiation Exercise

Objectives: To examine PPP negotiation.

Background: Two ISDN routers have started up and are negotiating various communication parameters for the BRI.

1. **Load** the trace file C:\SYCAP\TC107\PPP-NAK2. Press **F3** twice to display the data. Press **F6** for Display Options, enable **Two-Station Format**, **Detail** window, and set the **Name Width** to 13. Press **F3** to display the data.

2. Frame 1 is a PPP LCP Configure Request from the local router, DTE.B1, to the remote router, DCE.B1. **Tab** into the Detail window and you should notice Option Types 1, 3, 4, 5, 7, 11, and 17 being requested by DTE.B1.

PPP Negotiation Exercise

Continued

3. Press **F8** to advance to the next frame. Which option type is rejected by DCE.B1?

4. In the subsequent frame, we see DTE.B1 change its Option Type data to match that of DCE.B1. Does DCE.B1 acknowledge (Ack) or negative acknowledge (Nak) the new request?

5. Press **F8** to go to frame 5. This time we see DCE.B1 issue the PPP LCP Configure Request. Does DTE.B1 ack or nak the request in frame 6?
   Which Option Type is renegotiated in frame 7?
   How is the new request data different from the original?

PPP Negotiation Exercise

Continued

6. In frame 8, does DTE.B1 Ack or Nak the new request of frame 7? Does this seem normal to you? Hint: look at the "logical" HDLC address acked in frame 4.

7. In summary, did the negotiation complete successfully? Both routers were from the same manufacturer. Is there a potential for a problem if they were from different manufacturers?

Summary

- PPP defines a standard encapsulation scheme for the transport of different Network Layer protocols.
- It works over synchronous, asynchronous, dial-up, or dedicated lines.
- There are no restrictions on type of signaling employed or line speed.
- Link configuration, link termination and link maintenance frames are used to control PPP sessions.

Integrated Services Digital Network (ISDN)

Objectives

On completion of this section you will:

- Know the types of ISDN channels.
- Understand the user-network interfaces and functional groups.
- Understand the difference between Primary Rate and Basic Rate Interfaces.
- Know the types of switched circuits available.
- Recognize the functions of the D Channel.
- Understand the call setup and release procedures.
- Realize the internetworking value of ISDN.

ISDN Overview

- **Definition**: A full services, digital, end-to-end network
- Broadband-ISDN is a general networking concept for the evolution of various communication strategies that include N-ISDN, MAN, FDDI, SMDS, SONET and ATM.
- It uses SONET fiber (STS-96: 4.96Gbps) as the transport medium. It provides a single network for both circuit switched mode (voice and video) and packet switched mode (data, image) with ATM as the switching fiber.
- B-ISDN will be able to support all data types including high-bandwidth applications (150 - 600Mbps) like high-resolution graphics images and interactive video.

SNIFFER® UNIVERSITY

ISDN Concepts 9 - 3

Internetwork Analysis and Troubleshooting, 10/96, Rev. 5.0

Network General

- ISDN offers high-speed digital data transmission, and the ability to send and receive voice, data, still and moving images through the same fully digital connections.
- It is also a communications standard accepted throughout the world, which means that voice and high-speed data connections to most of the major business centers of Europe and the Pacific Rim are literally no more than a simple, dialed phone call away.

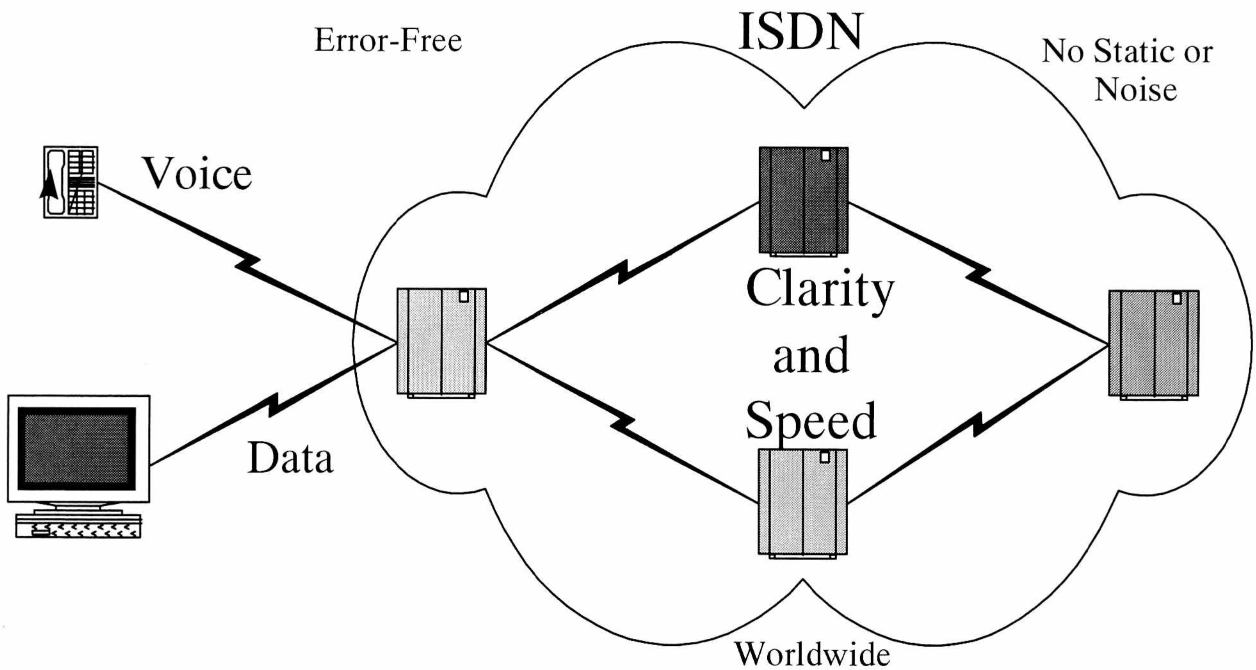
ISDN Principles

1. Support voice and non-voice in the same network
2. Support switched and non-switched applications
3. Transmission is based on the 64K (T1-DS0) connection
4. The network will offer intelligent switched services
5. A layered protocol will be used to access the network
6. ISDN will be offered in a variety of configurations

- The ISDN is based on six principles defined by the CCITT (Consulting Committee for International Telegraph and Telephone), now called the ITU (International Telecommunications Union).
- These principles were defined to help keep the services, features, and configurations of ISDN consistent internationally.

The Foundation for ISDN

Integrated Digital Switching for Voice and Data



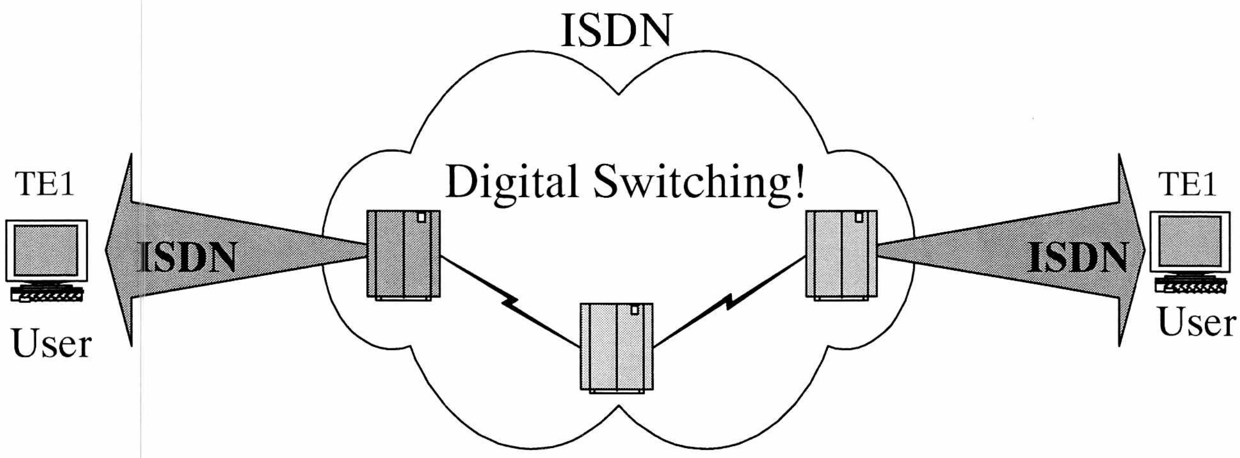
SNIFFER® UNIVERSITY

ISDN Concepts 9 - 5
Internetwork Analysis and Troubleshooting, 10/96, Rev. 5.0

Network General

- Two basic reasons why digital switching is important: clarity and speed.
- Digital signals ignore the static and noise that often affect analog transmissions, especially over long distances and older telephone lines, producing connections of the highest possible quality.
- They offer quiet, static-free voice conversations, and virtually error-free data connections, worldwide.
- The "I" in ISDN stands for integrated and refers to the simultaneous carrying of digitized voice, data, fax, and video in the same digital network.
- The integration of voice and data in a single digital switching environment results in a unique set of features the carrier can now offer to the user.

ISDN's Evolution



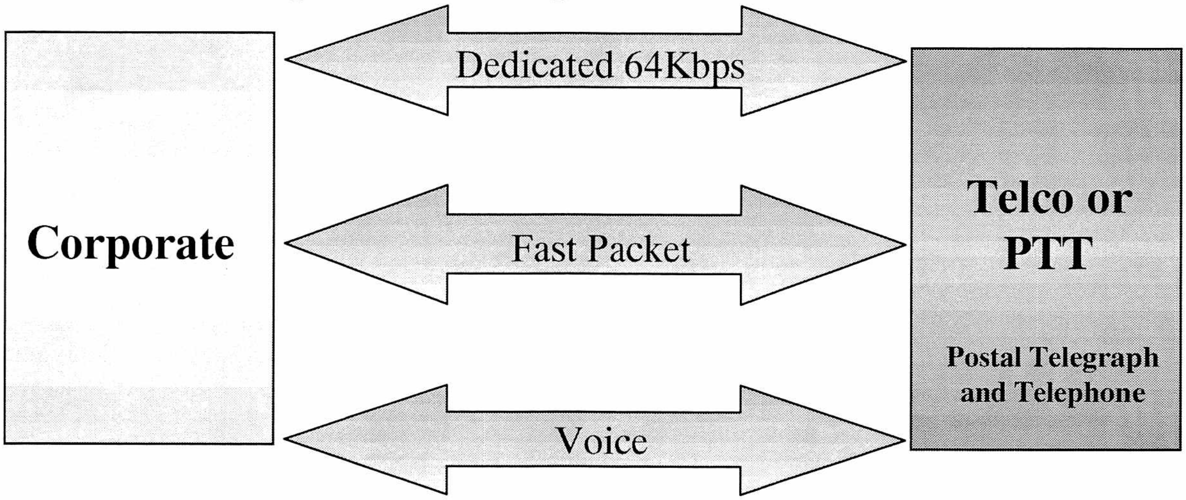
Extending the Digital Service out to the User

- The extension of the digital links to network subscribers is an essential part of ISDN.
- It is not sufficient that the internal transmission and switching facilities of the network be digital. To provide the wide range of digital services that ISDN offers, the link between the network subscriber and the network switch, also known as the digital subscriber loop must be digital.
- This digital extension from the network switch to the subscriber is ISDN.

Why is ISDN so Important?

Before ISDN

Separate point-to-point access lines required for separate functions

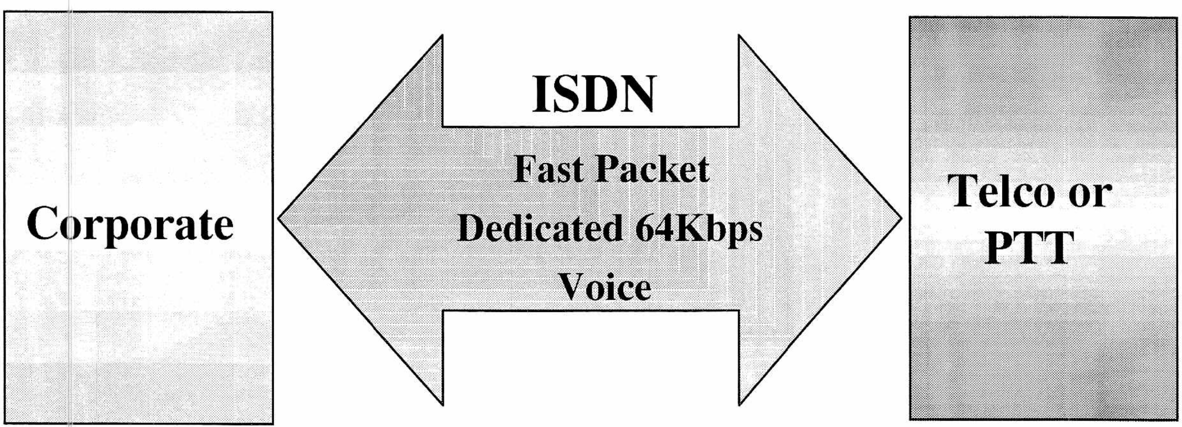


- Separate circuits dedicated to separate applications are very expensive to maintain.
- Unfortunately, this is how many users design their networks. A separate T1 or E1 circuit dedicated for voice, while another digital circuit dedicated for routed data, and finally a clear 64Kbs dedicated circuit installed for nightly backups.
- Organizations that keep close watch over every bit of bandwidth on primary lines can find themselves lavishing as much money on backup circuits that sit idle most of the time.

Why is ISDN so Important?

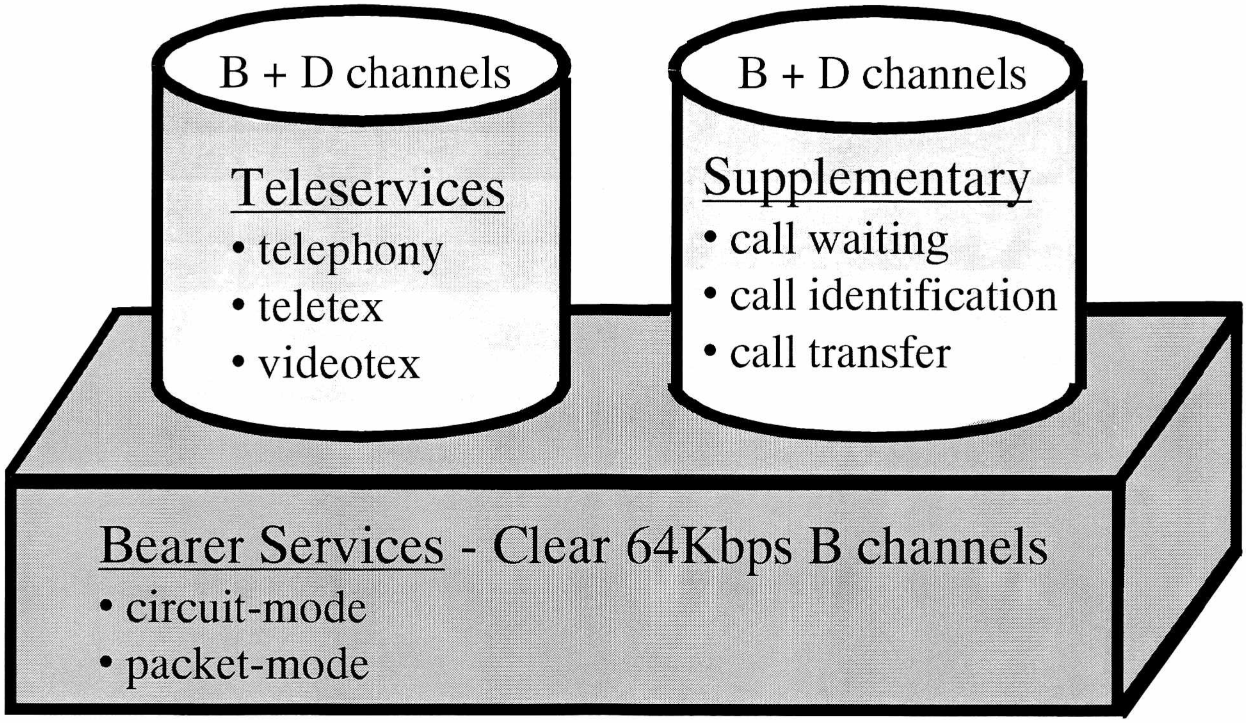
After ISDN

Single access line for separate functions



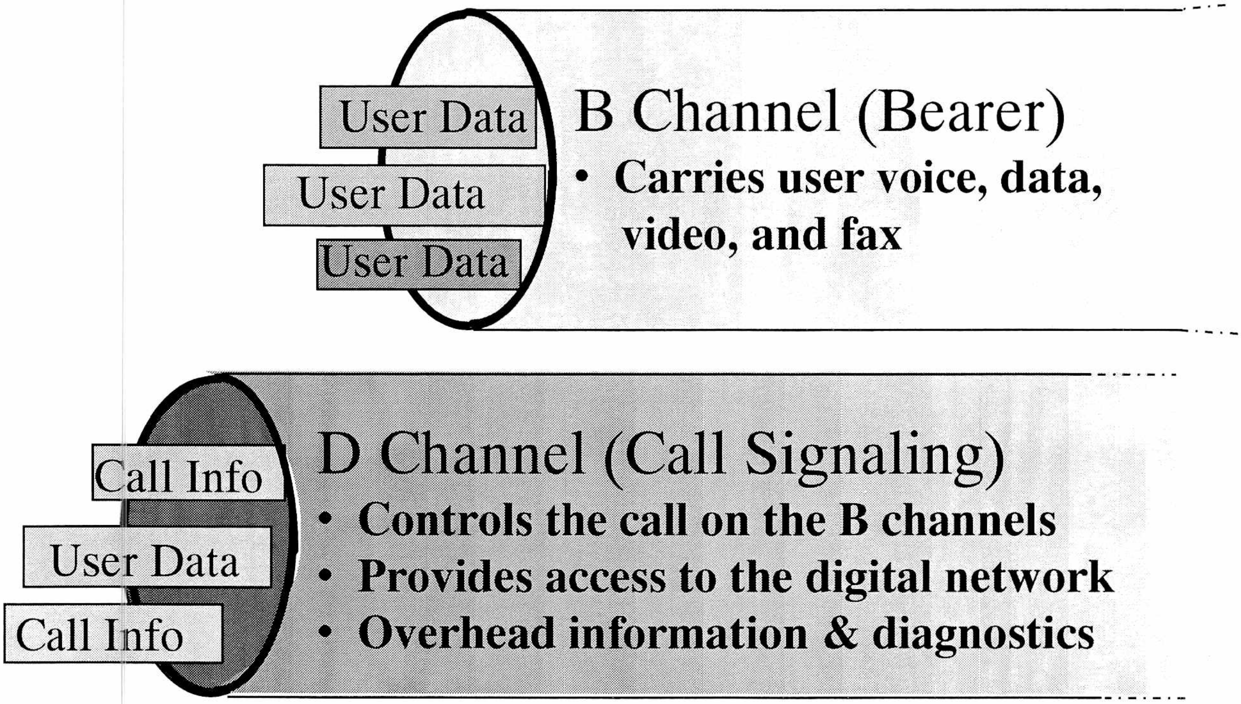
- One of the main advantages of ISDN is the ability to consolidate multiple traffic streams from different applications onto one digital circuit.
- Instead of three separate circuits to accommodate three different types of applications, ISDN makes it possible to use only one circuit. The result is a substantial cost savings.

ISDN Services



- The "S" in ISDN stands for "services" which refers to the three types defined by the ITU: bearer services, teleservices, and supplementary services.
- Bearer services provide the means to convey information (speech, data, video, fax etc.) between the users in real-time. These services are well developed. Bearer services are the foundation for which all other services will be carried out, thus the name" bearer" or B channels.
- Teleservices cover applications which are in the nature of terminal-service applications such as file transfers and document architecture. These services are significantly less developed than that of the bearer services. These services are carried out over both the B channels and the D channel.
- Supplementary services are always associated with a bearer service or teleservice. Both bearer services and teleservices may be enhanced by supplementary services. Like teleservices, these services are also carried out over both the B channels and the D channel.

Two Types of ISDN Channels



SNIFFER® UNIVERSITY

ISDN Concepts 9 - 10

Internetwork Analysis and Troubleshooting, 10/96, Rev. 5.0

Network General

- The digital pipe between the carrier (a.k.a. Telco) and ISDN subscriber is used to carry a number of communication channels. The capacity of the pipe, and the number of channels carried may vary from user to user.

B Channels

- 64Kbps clear channels.
- Can carry digitized voice, data, video, and fax.
- Can be used for circuit-switched or packet-switched.
- Rate adaptation available for multiple lower speed applications.

- Also called the *bearer channel.*
- The bearer channel is defined to carry out the bearer services.
- The B channel is a user channel that can carry digital data, PCM-encoded digital voice, or a mixture of lower-rate traffic. There are no protocol or other restrictions for B channels; they are simply transparent, circuit-switched, 64Kbps connections.
- There are two kinds of connections that can be setup over a B channel; circuit-switched and packet-switched calls. These connections are also known as bearer services. Bearer services are explained later.
- The designation of 64Kbps as the standard user channel rate was chosen as the most effective for digitized voice. However compression devices can shrink voice calls to 8Kbps or less making it possible to combine multiple voice calls into one B channel connection.

D Channel

- Sets up high priority real-time connections, maintains, monitors, disconnects, and reports connection problems on the B channels.
- The D channel also supports X.25 packet data and point-to-point applications to 16Kbps (for BRI).
  - Low priority non-time sensitive processes
  - Small file transfers
  - Transaction processing
  - Remote telemetry
- (We'll look at the D channel in more detail later.)

- Also called the *data or call signaling channel.*
- The D channel serves two main purposes. It carries common channel signaling information to control circuit-switched calls on associated B channels at the user-interface.
- In addition, the D channel may be used for packet-switching or low-speed (e.g. 100bit/sec) telemetry at times when no signaling information is waiting.
- The D channel adds a new dimension to digital networking. The D channel provides an out-of-band common channel signaling facility for ISDN. *Common channel signaling* is a signaling method in which a separate channel conveys signaling information. This information is used to identify called and calling stations, setup connections, identify line and network status, and provide billing data.
- The D channel of the Basic Rate Interface (BRI) is a 16Kbps channel that is shared for signaling, low speed packet switched data, and telemetry.
- The D channel of the Primary Rate Interface (PRI) is 64Kbps channel that is used exclusively for signaling.

H Channels

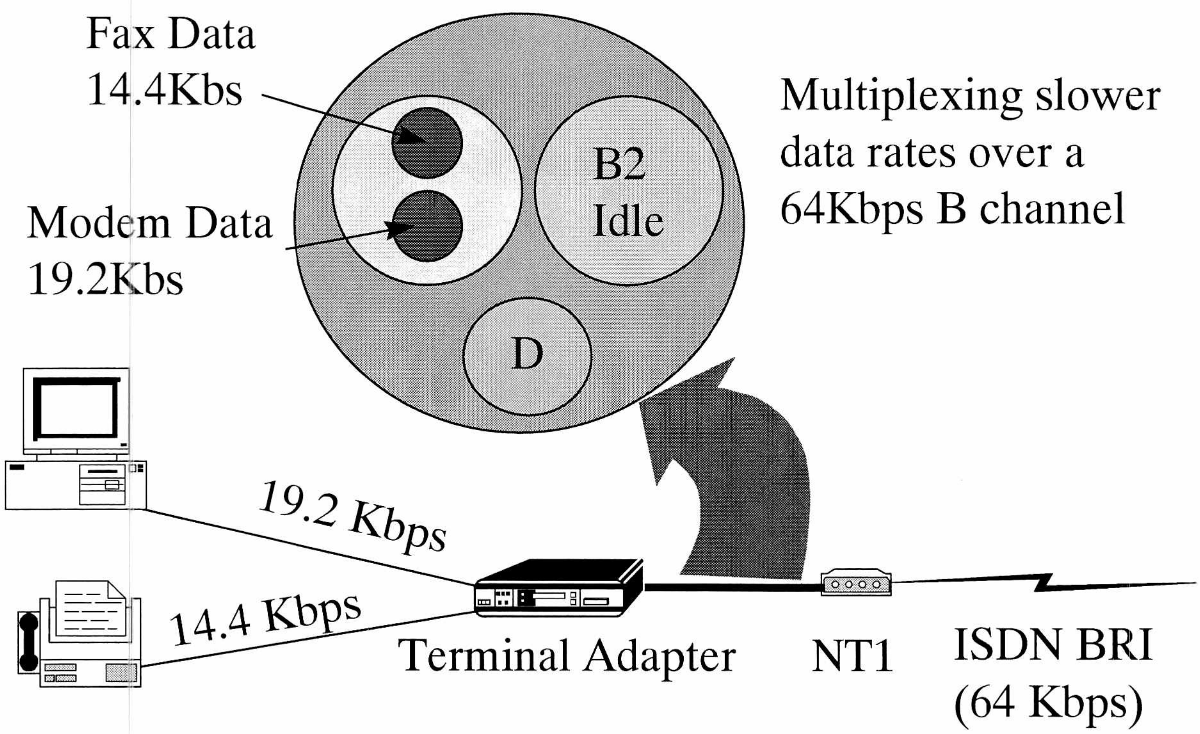
(A Combination of B Channels)

- Provided for user information at higher bit rates.
- Can be used for extremely time-sensitive data like video.
- The carrier determines the channel bandwidth options on dedicated mapped channels:
  - H0 = 384Kbs.
  - H11 = 1.544Mbs (US. and Japan).
  - H12 = 2.048Mbs (Europe).
- Used for video conference, inter-switch transport, and internet access.
- The timing is controlled by the network unlike PPP which is controlled by routers and assembly of frames.

- Also called the *high-speed or hyper* channel.
- H channels are provided for user information at higher bit rates. The user may use H channels as high-speed trunks for video conference calls, and back-up on demand links.
- H channels are grouped into transmission structures that are offered as a package to the user. These channels are called up as needed and are billed only for connected calls. This is a very economical method to attain high-bandwidth links on a call-by-call basis.

Asynchronous over ISDN BRI

V.110 and V.120 Rate Adaptation



SNIFFER® UNIVERSITY

ISDN Concepts 9 - 14

Internetwork Analysis and Troubleshooting, 10/96, Rev. 5.0

- Terminal adapters also perform a low level multiplexing function called rate adaption. Rate adaption refers to the ability of the TA to multiplex lower speed traffic into a high-speed 64Kbs B channel.
- Rate adaption is useful for low-speed applications that travel over ISDN like modem traffic, 14.4Kbs fax data, and 8or 16Kbps digitized voice.
- Two standards for rate adaption can be implemented: V.110 and V.120.
- Because rate adaption provides a way for low-speed traffic to access ISDN, it is not used for LAN-to-LAN applications over ISDN, but rather for home applications where the user wants to connect multiple low-speed devices to a single ISDN BRI circuit.

Key Points to Remember!

- ISDN is a digital technology.
- ISDN benefits customers by carrying multiple traffic types on a single digital circuit.
- ISDN is cost effective for varied types of data applications.
  - Daytime can be used for phone, evenings for data.
- The two basic ISDN channel structures are:
  - B channels for user data.
  - D channels for call signaling (call setup and teardown).
- H channels are grouped combinations of B channels.
  - Used for high-speed applications.
- Asynchronous data can be multiplexed onto a 64Kbps B Channel using rate adaptation schemes, but is not cost effective.

ISDN User-Network Interfaces

- Functional Groups - specific functions which may be needed to access ISDN.
  - Synchronization including, bit timing, multiplexing, protocol handling.
  - Example: Terminal Adapters, ISDN Routers, physical layer diagnostics using S bits.
- Reference Points - define the physical interface between the functional groups.
  - Example: R interface, S/T interface, U interface.

- To define the requirements for ISDN user access, an understanding of the user premise equipment and the necessary standard interfaces is critical.
- The principal motivation for the 7-layer OSI architecture is that it provides a framework for standardization. Once the functions to be performed in each layer are defined, protocol standards can be developed at each layer. This effectively organizes the standards work and provides guidance to software and equipment providers. By defining the services that each layer provides to the next higher layer, work in each layer can proceed independently. So long as the interface between two layers remains the same, new and different technical approaches can be provided within one layer without impact on neighboring layers.
- In the case of ISDN, the architecture on the subscriber's premises is broken up functionally into groupings separated by reference points. This permits interface standards to be developed at each reference point. Again this effectively organizes the standards work and provides guidance to the equipment providers.
- With stable interfaces, the subscriber is free to procure equipment from different suppliers for various functional groupings.

ISDN Functional Components

NT1
Network Termination 1

- Terminates the ISDN line from Telco and the PTT.
- Provides power, and confirms synchronization between TE and NT1 (F states), for NT1 to the switch (G states) via the U interface.
- Provides user access to the ISDN circuit.
- Converts 2-wire into an 8-wire interface.

NT2
Network Termination 2

- Primary Rate applications only.
- Provides switching for voice, data, video, fax.
- Accepts the 8-wire interface from the NT1.
- Provides layer 2 and 3 protocol handling.
- Separates the S and T reference points.
- Terminates the ISDN line from the NT1.

TE
Terminal Equipment

- Terminates the ISDN line from the NT1.
- Provides user access to the ISDN circuit.
- Accepts the 8-wire interface from the NT1.
- Provides layer 2 - 4 protocol handling.
- 2 Types of TE:
  - TE-1, an ISDN device
  - TE-2, a V.35-POT's non-ISDN device

SNIFFER® UNIVERSITY

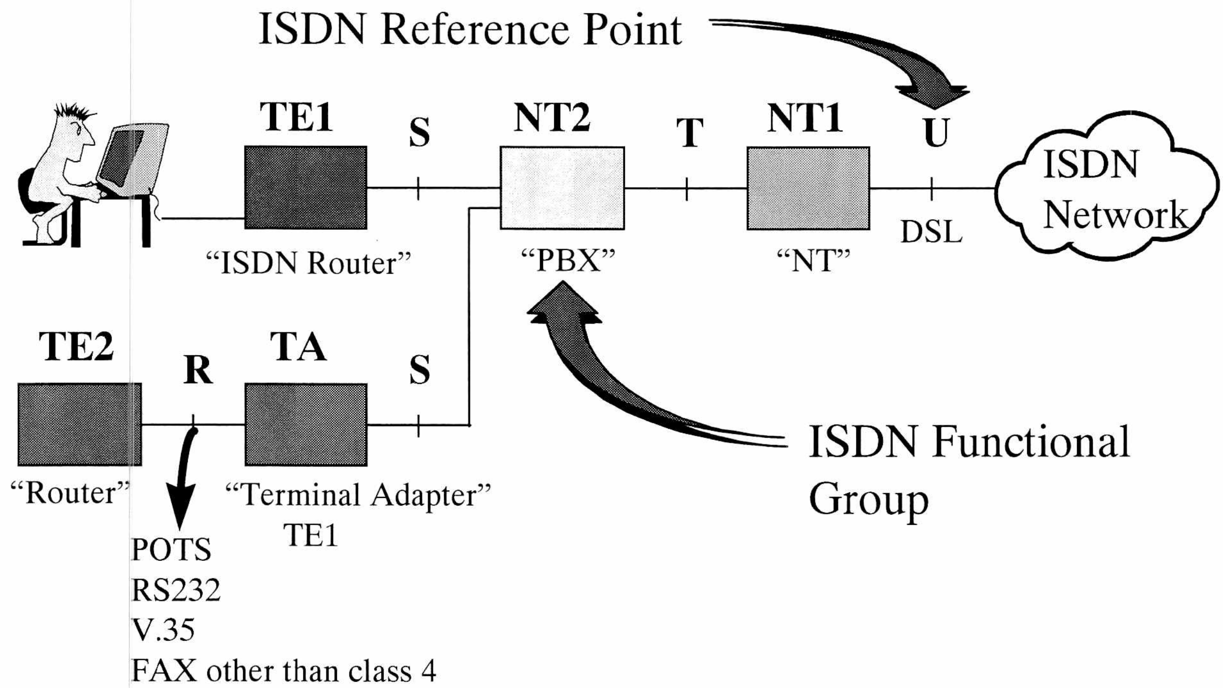
ISDN Concepts 9 - 17

Internetwork Analysis and Troubleshooting, 10/96, Rev. 5.0

Network General

- Functional groups are the components of the ISDN network such as the line termination, PBXs, and routers.
- The three functional components in an ISDN are the NT1, NT2, and TE.
- Under these groups are specific functions that are required to complete a subscriber's ISDN configuration.
- Because the group's functions are well defined it is easy to equate a network device to a functional group.
- For example, bridges and routers are defined as terminal equipment (TE), and a PBX is defined as a NT2.
- NT1 - Basic, NT2 - Primary
- NT1 - U interface, NT2 - S/T interface

ISDN Functional Groups and Reference Points for Primary Rate Access

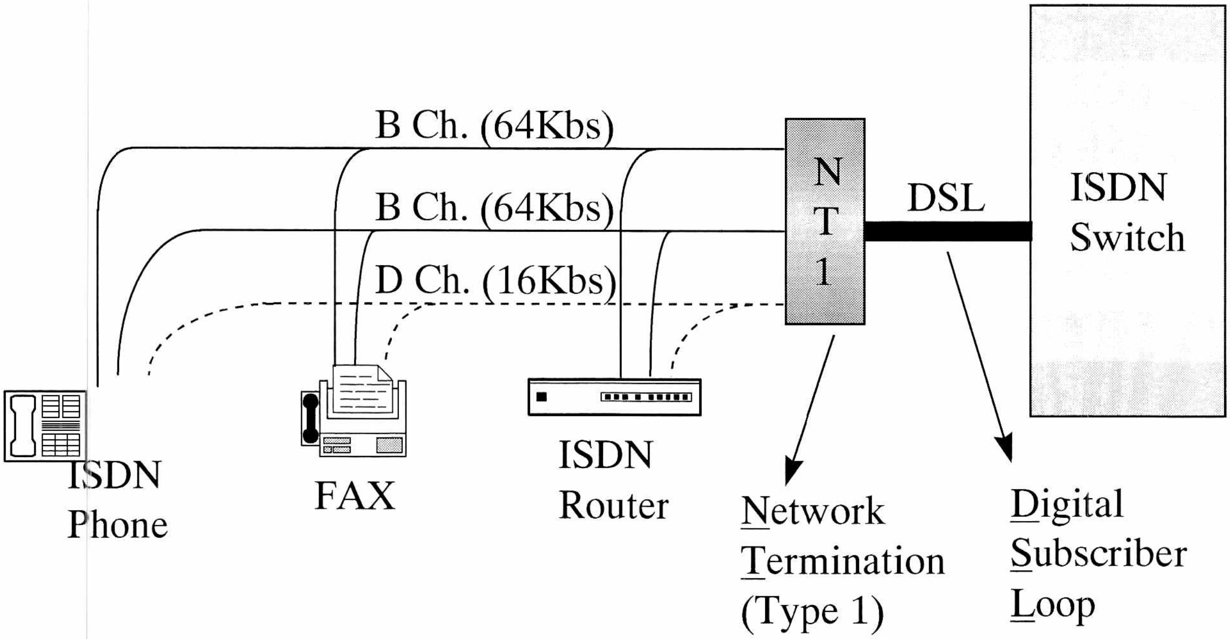


- Similar to the ISO model, the ISDN user-network interface provides a framework for standardization.
- This graphical representation shows how the functional groups (network devices) and reference points (access points) are related.
- As seen here, the functional groups represent specific network devices. With stable interfaces, the subscriber is free to procure equipment from different suppliers for the various functional groupings.
- The reference points separate the functional groups, but more importantly provide access points into the customer's ISDN premise equipment.
- Three new functional groups are introduced here; the Terminal Equipment (TE1, TE2), and TA.
- TE1 - refers to devices that support the standard ISDN interface such as digital phones, ISDN router, or a digital fax machine.
- TE2 - refers to devices that do not support ISDN interfaces such as routers with an RS-449 interface, X.25 terminals with V.24 interfaces. These devices require a terminal adapter (explained below) in order to connect to ISDN.
- TA - refers to a device that converts non-ISDN interfaces to ISDN and vice versa. These devices are similar to modems, in that they provide the necessary interface to the network.
- NT1 stands for Network Termination Type 1 and separates the PTT network from the user's network.
- R, S, T, and U are interfaces. TEx, NTx are devices.

ISDN Interface Circuits

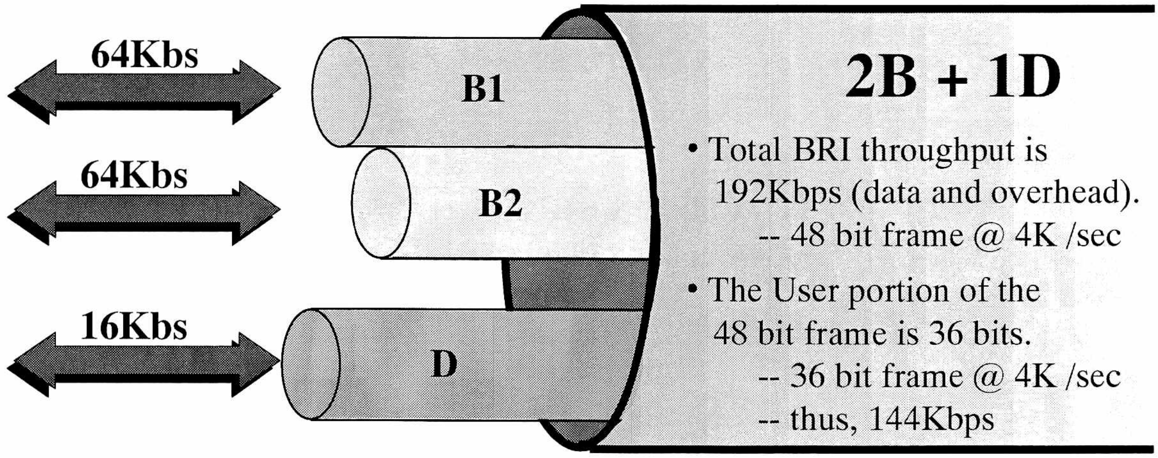
- Basic Rate Interface Pipe
  - 2 B and 1 D channel
  - **The Sniffer will look at both Bs and D, time correlated**
- Primary Rate Interface Pipe
  - Up to 23 B channels and 1 D channel analysis (T1)
    - Used in the United States, Canada and Japan
  - 30 B and 1 D channels (E1)
    - Used in Europe

Basic Rate Interface (BRI)
Point-to-Point or Multi-Point



- In a Basic Rate Interface (BRI) configuration you can connect one device (point-to-point) or connect up to eight devices (multi-point), each with their own **phone numbers**. It is possible to have up to 16 different phone numbers on a single BRI. The latter implementation is called a *passive bus* configuration.
- Each device that is connected to the BRI has access to two 64Kbps B channels and a single 16Kbps D channel. This shared environment is ISDN's advantage over other technologies.
- When a device makes a call to a remote device, it will access the D channel and proceed to establish a B channel connection.
- The "NT" refers to a "network termination", or a point where the PTT will terminate the ISDN circuit.
- The "DSL" refers to the "Digital Subscriber Loop". It is the digital extension from the network out to the user. The DSL in this case is a ISDN BRI circuit that runs over two wires, just like the traditional telephone wires.
- The "ISDN Switch" is located at the PTT. It accepts digital ISDN circuits from literally thousands of users. It's primary function is to provide the switching functions for every individual end-user that is connected.

The Basic Rate Interface "Pipe"



128Kbps	total B channel bit rate (2B ch.)
+ 16Kbps	D channel
144Kbps	total user bandwidth

SNIFFER® UNIVERSITY

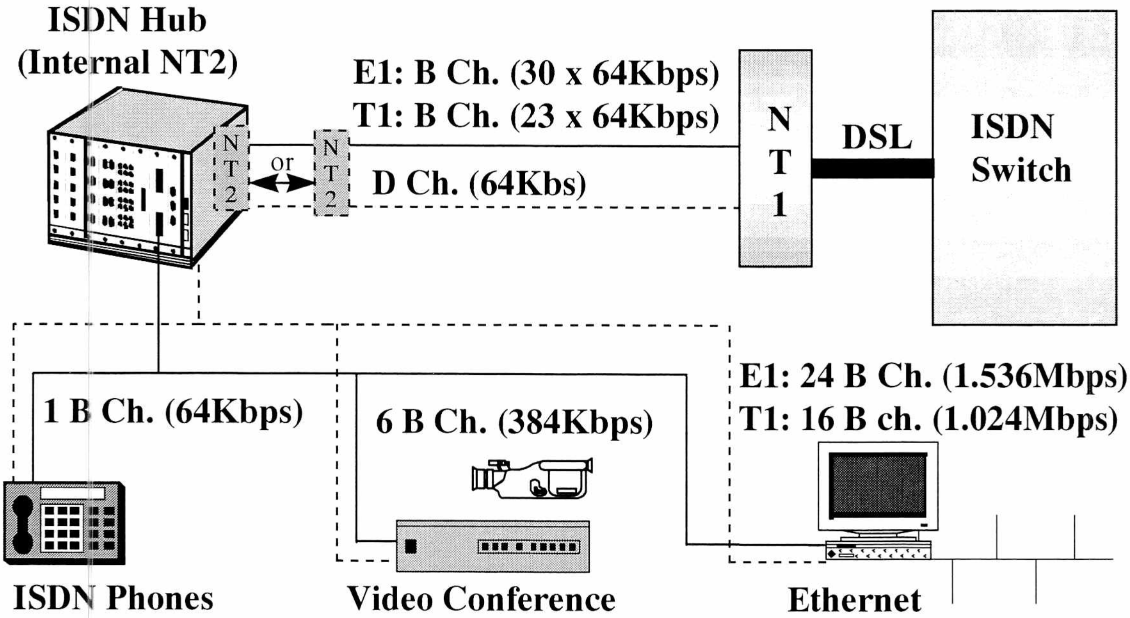
ISDN Concepts 9 - 21
Internetwork Analysis and Troubleshooting, 10/96, Rev. 5.0

Network General

- ISDN BRI consists of two full-duplex 64Kbps B channels and a full-duplex 16Kbps D channel. The total bit rate, is 144Kbps.
- However, framing, synchronization, and other overhead bits bring the total bit rate on a basic rate access link to 192Kbps.
- In some cases, one or both of the B channels remain unused. This results in a B + D (1B+D) or just a D interface (0B+D) rather than 2 B + D configuration. In these configurations, the unused B channels are filled with 1s.

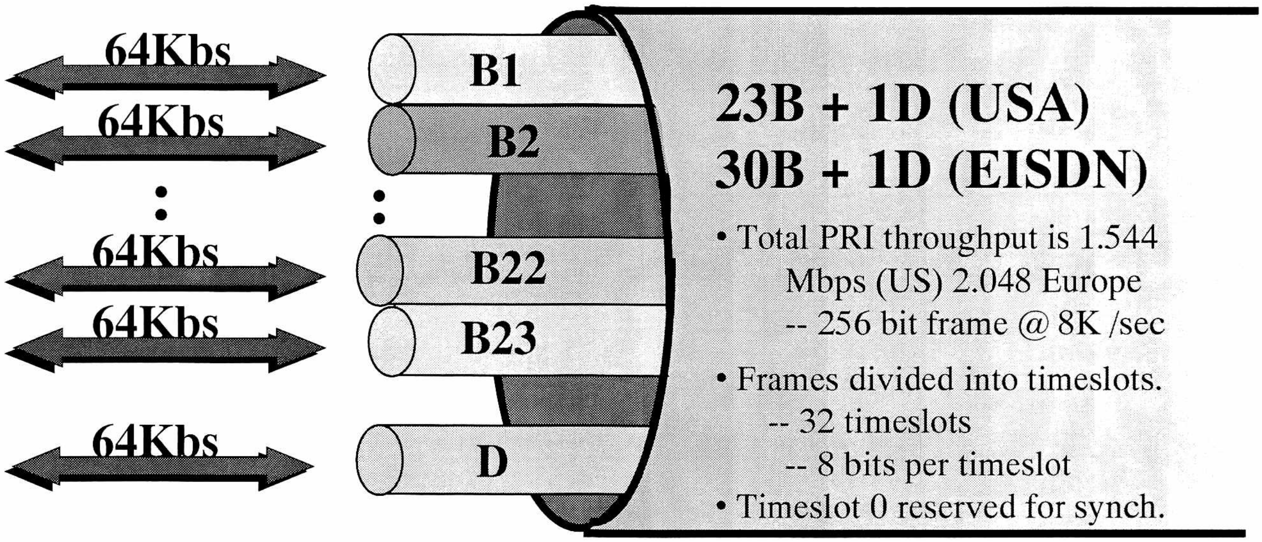
Primary Rate Interface (PRI)

Point-to-Point Only



- This slide shows a European PRI implementation with 30 B channels and the D channel.
- In a PRI configuration only a single device can have access to the circuit, this is known as a point-to-point configuration. This single device connected to the PRI is commonly used as a "front-end" accepting connections from other devices.
- Primary Rate is intended for users with greater capacity requirements, such as offices with a digital PBX, video conference codec or a LAN.
- The digital subscriber loop (DSL) for a PRI can either be a T1 circuit (US.) or a E1 circuit (Europe).
- The "NT" differs from that of a BRI NT. The primary purpose of the NT in a PRI environment is to terminate the digital circuit from the PTT. Since a PRI is really ISDN over E1, the NT closely resembles a CSU (channel service unit). In addition to terminating the PRI circuit, the NT also provides low-level line conditioning.
- A common PRI configuration is to have an ISDN bandwidth aggregator or an ISDN "hub" control the PRI bandwidth. This device accepts connections from other devices such as a PBX, video conference codec, and a LAN. It's main purpose is to provide bandwidth on demand for any of the connected devices.
- This configuration is very flexible, as only one circuit (PRI) is needed to connect multiple devices through a bandwidth aggregator.

The Primary Rate Interface "Pipe"



- Because of the digital transmission hierarchies used in different countries, it was not possible to standardize on a single data rate.
- The US., Canada, and Japan make use of a transmission structure based on 1.544Mbps (T1), in Europe 2.048Mbps (E1) is the standard rate.
- The channel structure for the 1.544Mpbs rate is 23 B channels plus one 64Kbps D channel.
- The channel structure for the 2.048Mbps rate is 30 B channels plus one 64Kbps D channel.
- In some PRI configurations, it is possible to have PRI with all B channels and no D channel for signaling. When no D channel is present, it is assumed that a D channel on another PRI at the same subscriber location will provide the signaling.

Basic Rate vs. Primary Rate

	Basic Rate	Primary Rate
User Bit Rate	128 Kbps	1.472 Mbps - 23B (US. and Japan) 1.920 Mbps - 30B (Europe)
Signaling Channel	16 Kbps - D	64 Kbps - D
Bearer Channels	64 Kbps - B optional for PVC	64 Kbps - B 384 Kbps - H0 1.544 Mbps - H11 (US. and Japan) 2.048 Mbps - H12 (Europe)
Channel Formats	2 B + D*	23 B + D (US.) , 30 B + D (Europe)* 24 B (US.) , 31 B (Europe)* 2 H0 + 11 B + D (US)*

*Depends on Telco provider or switch manufacturer.

Source: I.411, T1S1 Standards

- Two distinct ISDN interfaces provide the customer with flexible configurations.
- BRI for remote users who need access to the corporate backbone, and PRI located at the corporate site typically connected to a PBX.
- Key points to remember:
  - Primary Rate Interface is a point-to-point configuration.
  - Basic Rate Interface is point-to-point and multi-point.
  - ISDN BRI throughput is 144 Kbps (2B + D).
  - European ISDN PRI throughput is 1.984 Mbps (30B + D).
  - Non-European ISDN PRI throughput is 1.536 Mbps (23B + D).

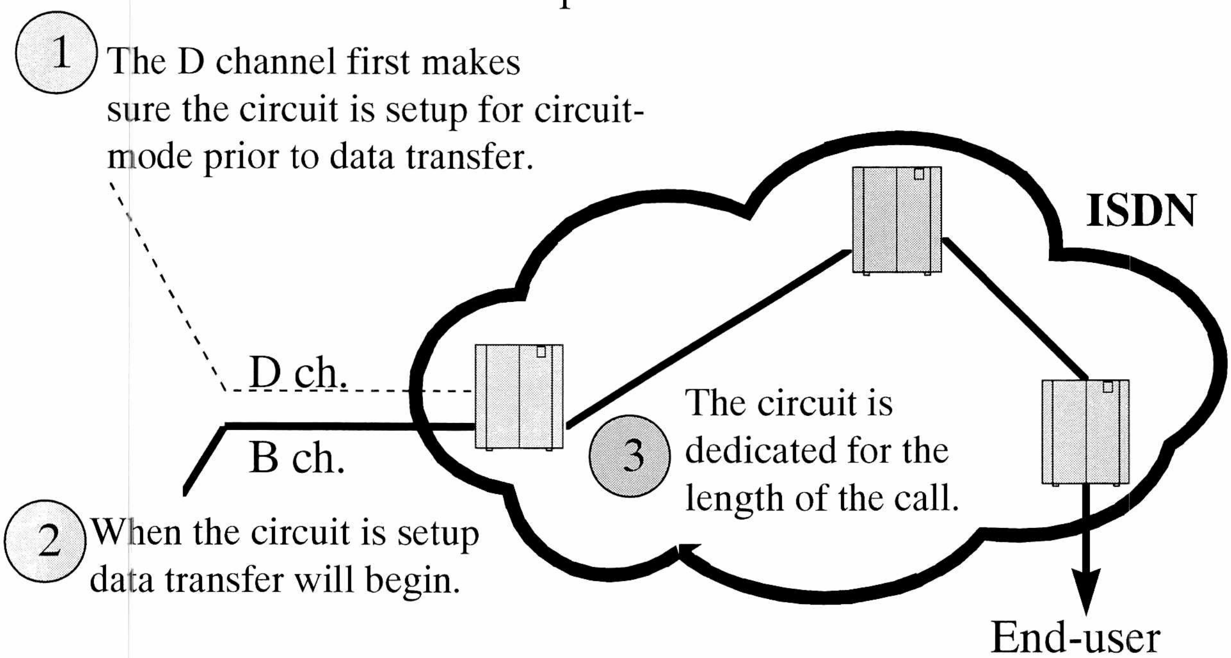
ISDN Switching

- The two basic ISDN connections
  - Circuit-switched for data and voice
    - Modulation techniques
      - Group 4 FAX
      - PCM Voice
    - Video Compression
      - Multipoint Point-to-point
  - Packet-switched for data only
    - Supports X.25 data

- ISDN provides three types of service for end-to-end connections:
- Circuit-mode or circuit-switched connections is used for voice and transparent data.
- Packet-mode or packet-switched connections are intended to support X.25 traffic, this service was defined primarily to connect to the world-wide X.25 network.

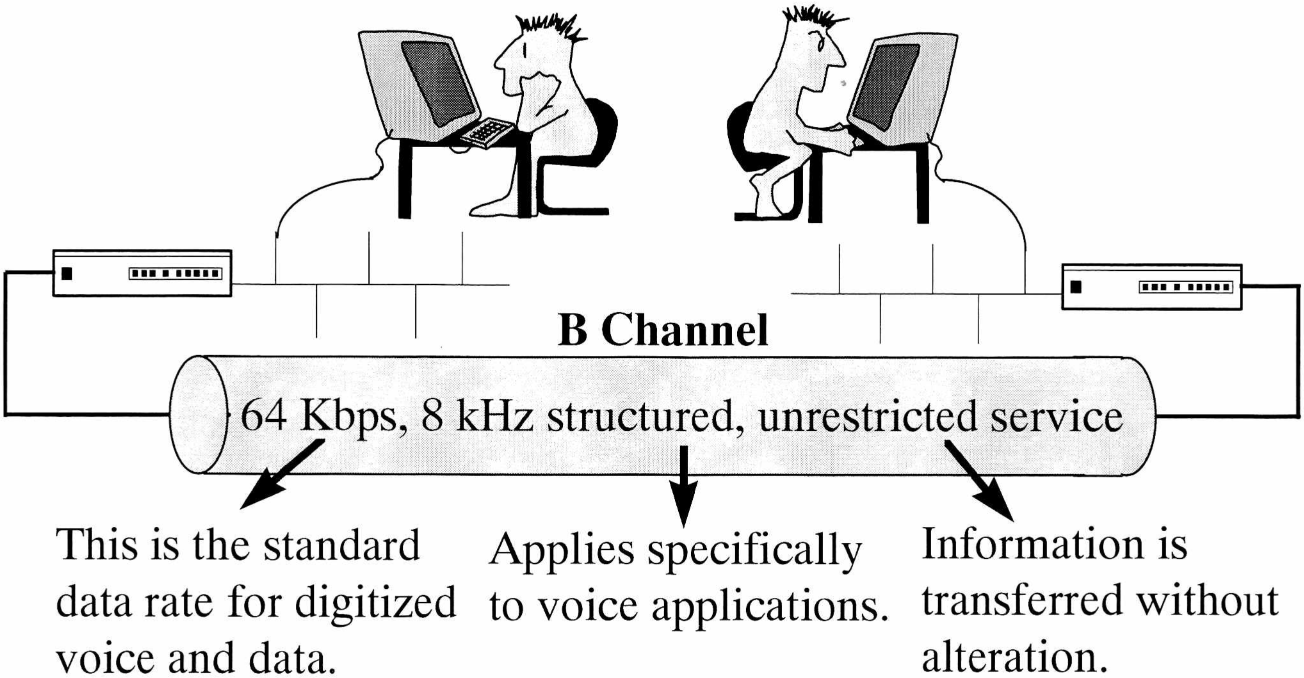
ISDN Circuit-Mode Connection

Signaling and user information are transmitted over separate channels.



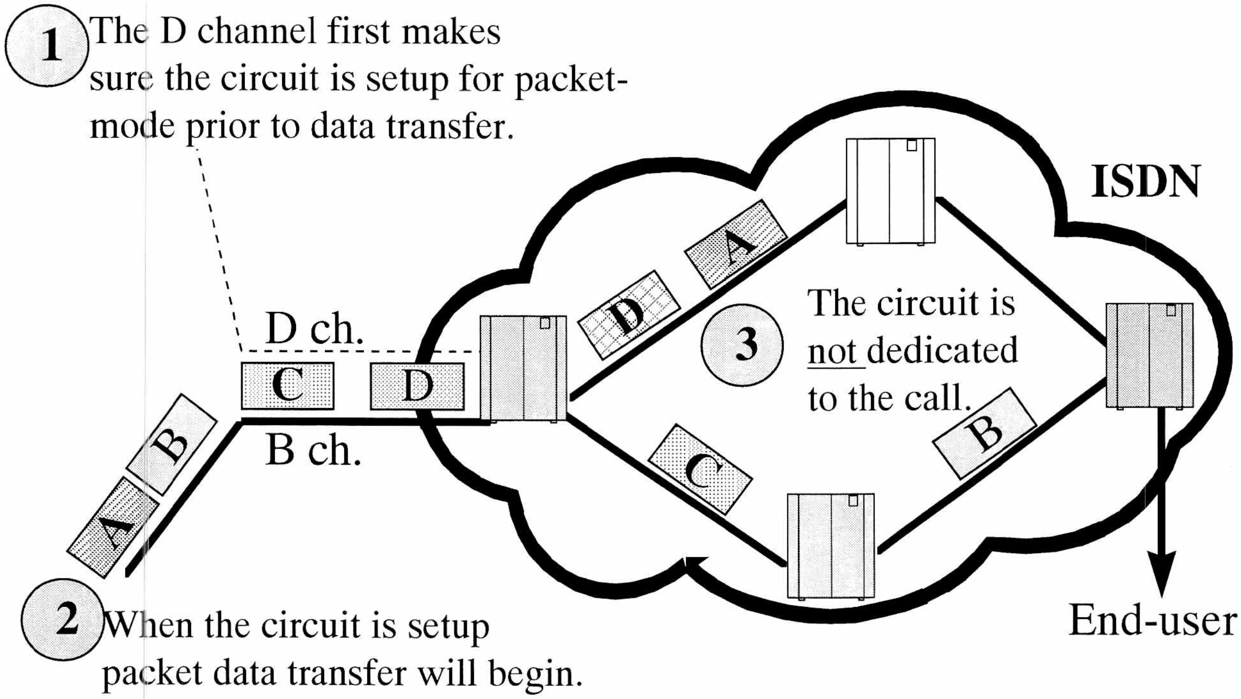
- The network configuration and protocols for circuit-switching involve both the B and D channels. The B channel is used for the transparent exchange of user data. The communicating users may use any protocols they wish for end-to-end communication. The D channel is used to exchange control information between the user and the network for call establishment, termination, and access to network facilities.
- The main attributes of circuit-switching are that the circuit is first established before data is sent, and it will remain dedicated for the duration of the call. This type of connection is very well suited for applications that are sensitive to delays such as voice and video conferencing.

The Circuit-Switched Connection



- The circuit-switched call is analogous to a dedicated "pipe" between two communicating users.
- The most common circuit-switched connection that is setup on an ISDN B channel is the 64Kbps, 8Khz structured, unrestricted service.
- The "64Kbps" data rate is the fundamental building block of ISDN services.
- The term "8Khz structured" means that, in addition to bit transmission, a structure is transferred between the communicating users. When one user transmits information to another user, the data is accompanied by 8Khz timing information. This information is important for speech transmission.
- The term "unrestricted" means that the information is transferred without alteration; this also known as a transparent bearer service. User may employ this service for any application that requires a data rate of 64Kbps.
- Unrestricted also means signaling is out of band (D channel).

ISDN Packet-Mode Connection



SNIFFER® UNIVERSITY

ISDN Concepts 9 - 28

Internetwork Analysis and Troubleshooting, 10/96, Rev. 5.0

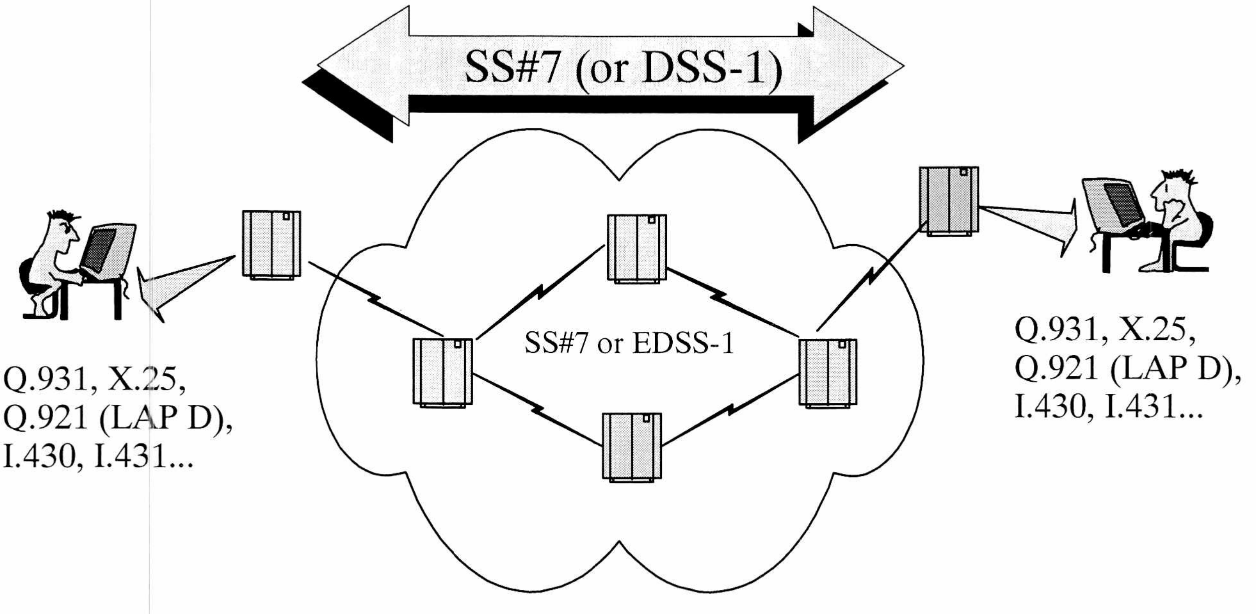
Network General

- Unlike circuit-switching, packet-switching allow dynamic sharing of the available WAN bandwidth. The packet data is addressed by the user and routed by the network.
- In a packet-mode connection, the D channel sets up a packet-switched call to the ISDN network. The ISDN network will then expect to receive X.25 packets from the user.
- The packets are routed to the end-user destination via X.25 addressing.
- The main attribute of packet-switching is that the circuit within the network is not dedicated for the duration of the call. Since every packet has an individual address, it can take several different routes to the same destination.
- A single B channel can be used to connect to the world-wide X.25 network at 64 Kbps.
- The D channel uses a packet-switched protocol for call signaling and user data.

ISDN D Channel Topics

- How telephony switching technologies like SS#7, DSS-1, relate to ISDN.
- The difference between in-band signaling and out-of-band signaling.
- How the LAP-D ANSI Q.921 (I.441) protocol works.
- Understanding TEIs and SAPIs.
- Understanding Q.931 (I.450/I.451) protocol messages.

ISDN Signaling Protocols

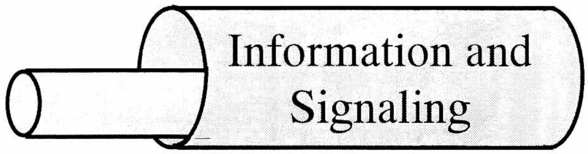


SS#7 (or EDSS-1) controls the path between the switches and will transparently reroute around problems.

- European ISDN end-to-end signaling is commonly referred to as the ISUP or ISDN Subscriber User Part.
- EDSS-1, or European Digital Subscriber Signaling System No. 1, is a user-to-network interface.
- SS#7 is the signaling system between PTTs, similar to EDSS-1 being the signaling system between the subscriber and the PTT. Most carriers will finish deploying SS#7 by the end of 1995. ISDN's advanced services need SS#7 support along the entire communication path to work.
- The overall purpose of SS#7 is to provide an internationally standardized common channel signaling system. Common channel signaling is a signaling method in which a single channel conveys, by means of special messages, signaling information.
- This information is used to identify called and calling stations, setup, maintain, release connections, and provide billing information.

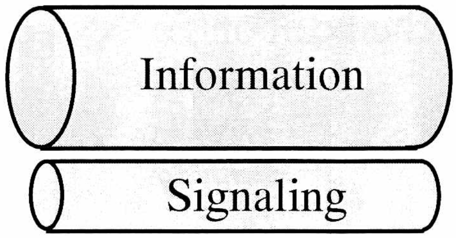
D Channel Signaling
In-Band vs. Out-of-Band

The Old Telephone Network



- Occupies the same channel as the user information.
- Adds overhead to information channel.

ISDN



- Allows for quicker call establishment.
- Shared by multiple users.
- Information bandwidth is not compromised.

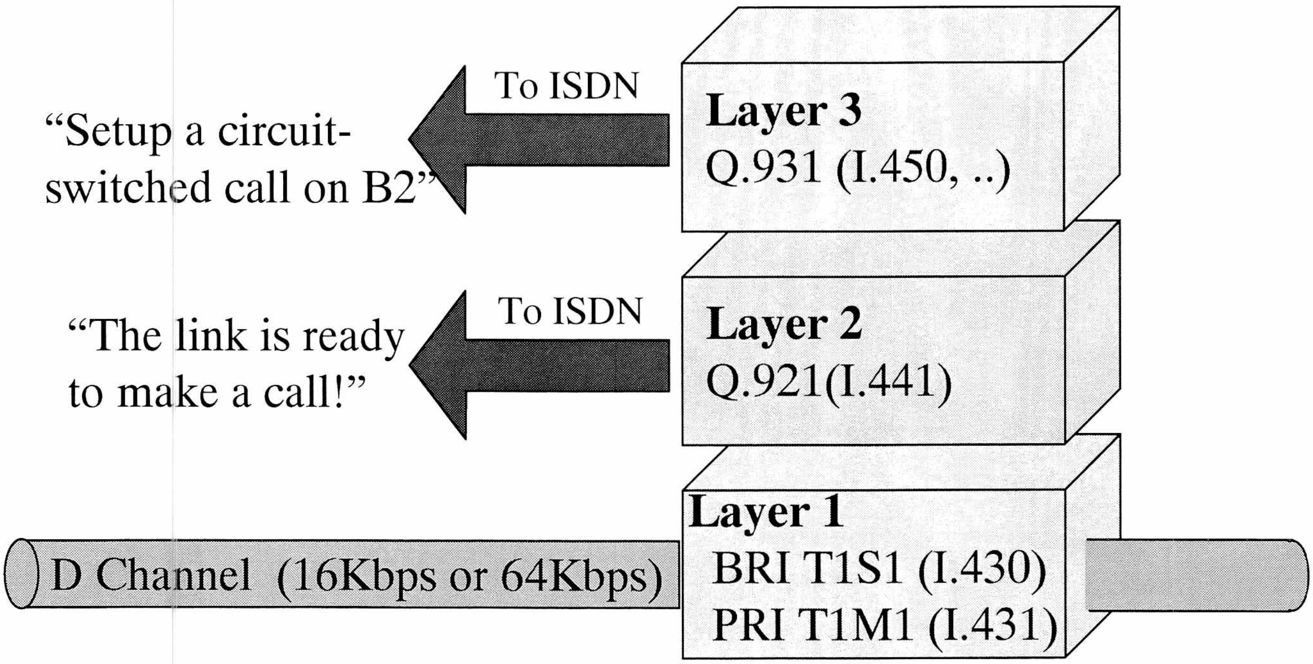
SNIFFER® UNIVERSITY

ISDN Concepts 9 - 31
Internetwork Analysis and Troubleshooting, 10/96, Rev. 5.0

Network General

- In the world of telephony, signaling refers to the process of establishing, maintaining, terminating, and accounting for a circuit-switched connection between two end-points. Currently, the most common signaling schemes are dial pulse (DP) and dual tone multi-frequency (DTMF). Both schemes employ an in-band signaling approach where signaling information occupies the same channel as the user information. This approach imposes an overhead burden and "robs" the user of the limited available bandwidth.
- The ISDN D channel provides a solution to this problem via a common channel signaling (CCS) approach.
- With CCS, all signaling information is carried out-of-band on a special signaling channel. This approach allows for quicker call setups and routing, as the setups and routing are performed over a separate high-speed digital channel.
- Further, this out-of-band signaling channel is shared by a number of user devices, thus eliminating the excessive overhead burden.

ISDN Layers



- The D channel is made up of the first three layers of the OSI model. In order to setup a B channel call a specific procedure is followed.

  1) Layer 1 must first be active (power to the line, synchronization).

  2) Layer 2 (LAP-D) establishes a logical link between the user device and the network device. The Layer 2 link needs to be setup so Layer 3 (Q.931) messages can proceed.

  3) Once Layer 2 is established, Layer 3 (Q.931) messages can now proceed.

  4) Layer 3 will follow a strict protocol procedure to request a B channel connection.

  5) Once the B channel connection is made, the user can now send data freely over the B channel.

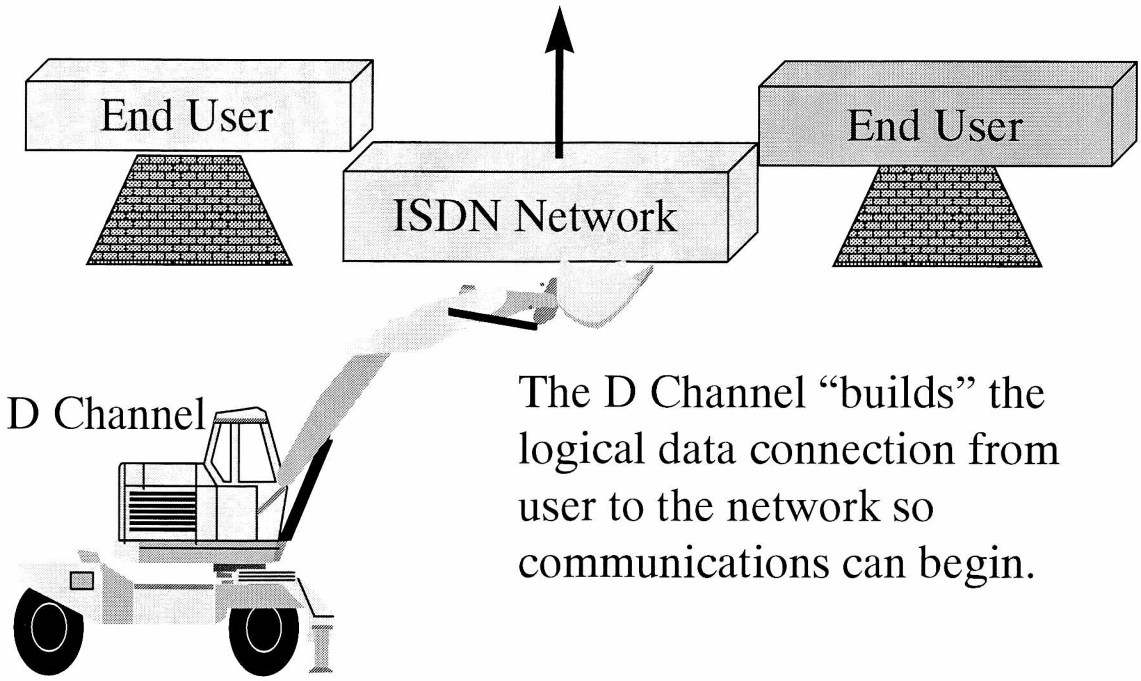
  6) When the user is finished sending data, Layer 3 sends a message to the network requesting to terminate the B channel call.

  7) The network obliges and tears down the B channel connection.

  8) Since Layer 3 is finished with the call, Layer 2 will begin to tear down the logical link.

- The D channel will remain idle, except for Layer 2 sequence and flow control information, until the user device wishes to make another B channel call.

The ISDN "Workhorse"



The D Channel "builds" the logical data connection from user to the network so communications can begin.

- The D channel protocols bring the out-of-band signaling approach to the users of ISDN-based networks.
- The D channel is the focal point of any ISDN B channel connection. It is responsible for building data connections from the user to the network.
- The D channel carries common-channel signaling information to control circuit-switched calls on associated B channels at the user interface.
- It is also used for packet-switching or low-speed telemetry (e.g. 100bps).

Q.931 (I.450, I.451) Messages

- Defines how the user and ISDN network communicate (Layer 3)
- Over 70 messages are defined to control:
  - Call Establishment
  - Call Information
  - Call Disconnection
  - Miscellaneous network functions

Information elements, or Layer 3 signaling messages, are grouped into three categories:

1) Call establishment messages - used to initially setup a call.

SETUP

ALERT

CALL PROCEEDING

2) Call information messages - are sent between the user and the network.

USER INFORMATION

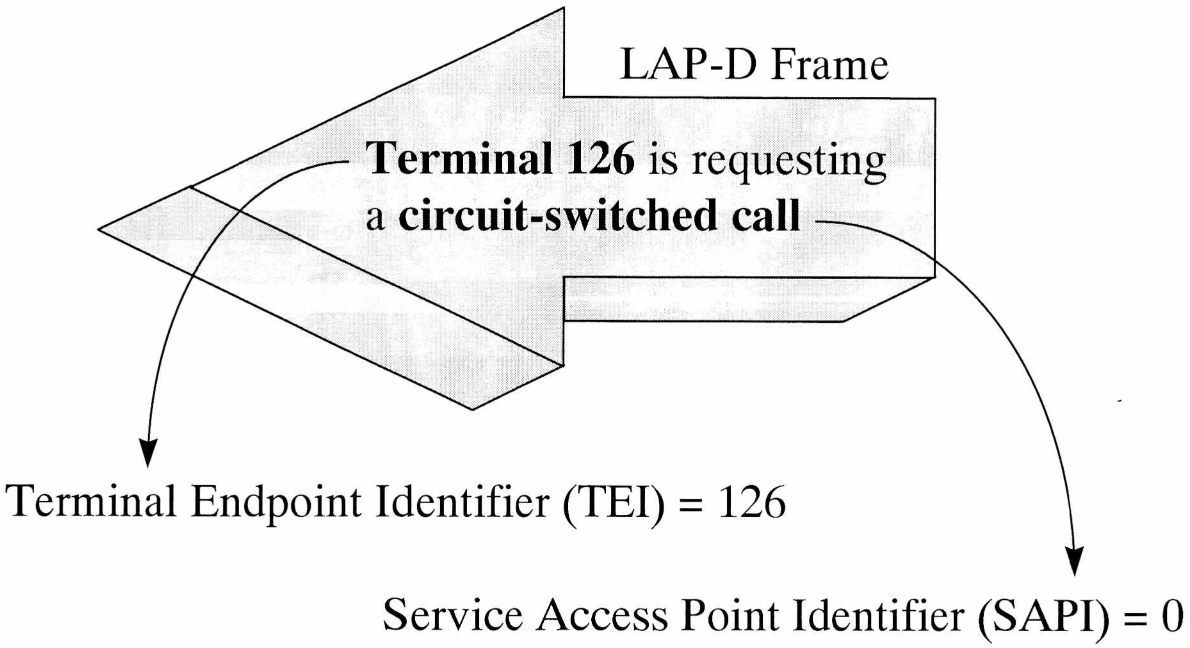
RESUME

3) Call termination messages - used to terminate a call.

DISCONNECT

RELEASE

Making the Connection
<u>L</u>ink <u>A</u>ccess <u>P</u>rotocol - <u>D</u> Channel



- LAP-D is also referred to as Link Access <u>Procedure</u> - D channel.
- LAP-D has to deal with two levels of multiplexing. First, at a subscriber site, there may be multiple user devices sharing the same physical interface. Second, within each user device, there may be multiple types of traffic (packet-switched data like X.25 and call signaling information).
- To accommodate these levels of multiplexing, LAP-D employs a two-part address consisting of a terminal endpoint identifier (TEI) and a service access point identifier (SAPI).
- Layer 2.

TEIs and SAPIs

- Identifies a unique terminal on the ISDN.
- TEIs are automatically assigned.

- Identifies a Layer 3 user of LAP-D.
- SAPIs are automatically assigned by the terminal for a specific type of service the B channel will carry.

- Typically, each user device has a terminal endpoint identifier (TEI). It is also possible for a single device to be assigned more than one TEI (e.g. terminal concentrator). TEI assignment are automatic when the equipment first connects to the ISDN line and are different each time the terminal is plugged into the ISDN network.
- The TEI values are determined prior to any Layer 3 messages being sent.
- The service access point identifier (SAPI) is used to identify the type of Layer 3 communication LAP-D will be carrying, such as:
    - Call control procedures
    - X.25 communication
    - Management procedures
- The SAPI values are determined prior to any Layer 3 messages being sent.

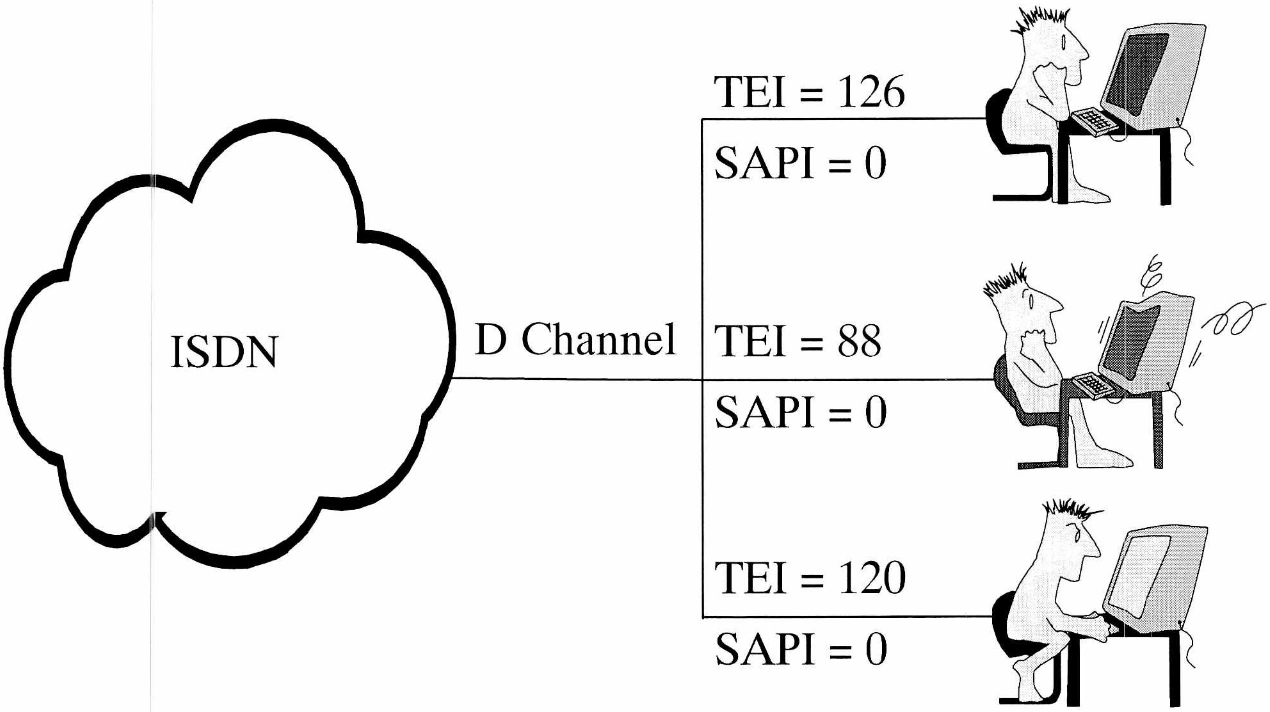
TEI and SAPI Assignments

TEI Values	Description
0 - 63	Non-automatic TEI assignment equipment
64-126	Automatic TEI assignment user equipment
127	Reserved

SAPI Values	Description
0	Call control procedures
1	Reserved for packet-mode communication
16	Packet communication via X.25 level 3
17	Terminal Loopback Test
63	Layer 2 management procedures
All others	Reserved for future standardization

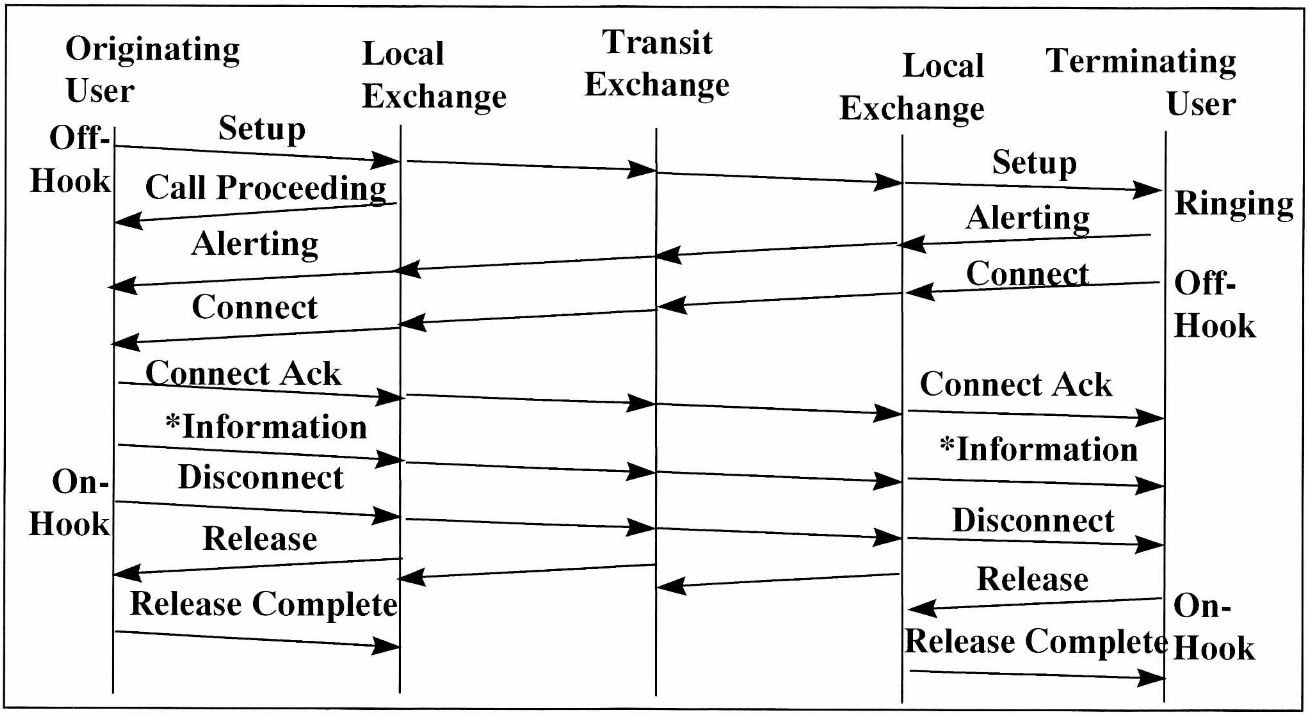
- TEI values are assigned dynamically and will always be unique. The terminal will "register" with the network and a TEI value will be assigned. This dynamic assignment by the network means these TEI values are different each time the terminal connects to the ISDN.
- When the logical link is no longer needed, the network will make sure the TEI is removed, unassigned or reassigned.
- SAPI values are assigned automatically by the terminal, it corresponds to a Layer 3 protocol entity within a user device.

Unique Connections = *TEI* + *SAPI*



- The SAPI values are unique with a TEI, that is for given TEI, there is a unique Layer 3 entity for a given SAPI.
- The TEI and SAPI together uniquely identify a logical connection.
- Sometimes the TEI and SAPI combination are referred to as data link connection identifiers (DLCI).
- At any one time, LAP-D may maintain multiple logical connections, each with a unique DLCI.
- Key points to remember.
- The LAP-D protocol is used to setup the data link connection.
- The TEI stands for Terminal Endpoint Identifier.
    - It is the "temporary name" of a user device.
- The SAPI stands for Service Access Point Identifier.
    - It "tells" the network what type of data the B channel will be carrying.

ISDN Call Process



*Information: addressing information (negotiation for resources) if not included in setup message.

SNIFFER® UNIVERSITY

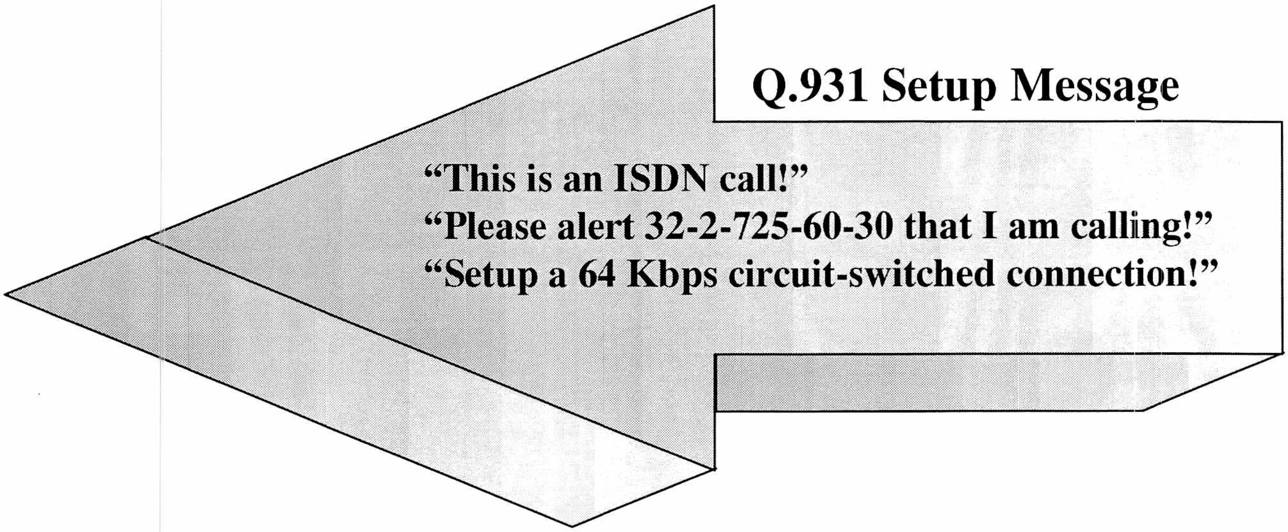
ISDN Concepts 9 - 39

Internetwork Analysis and Troubleshooting, 10/96, Rev. 5.0

Network General

- Layer 3 messages are used to setup a call between the originating and terminating customer premise equipment (CPE).
- There will be different vendor implementations of this process.

Establishing the Call
Q.931 (I.450, I.451) Messages

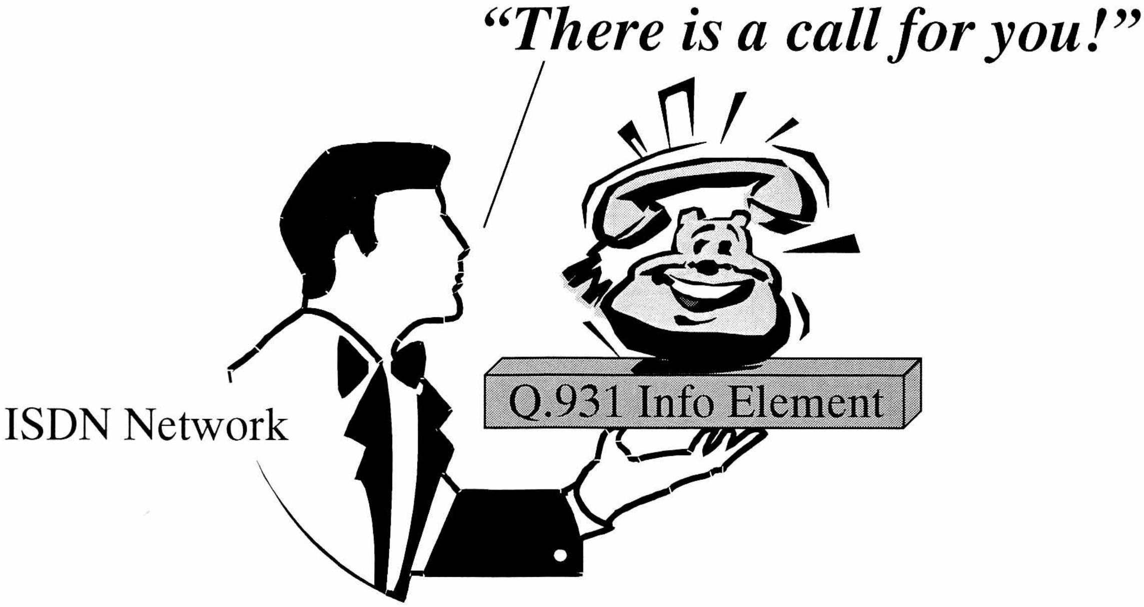


- For call control signaling the Layer 3 protocol, Q.931, specifies procedures for establishing connections on the B channel. It also provides user-to-user signaling over the D channel.
- The process of establishing, controlling, and terminating a call occurs as a result of control signaling *messages* exchanged between the user and the network over the D channel.
- A common format is used for all Q.931 messages, the three fields common to all messages are:
  - Protocol Discriminator - used to distinguish messages for user- network call control from other message types such as X.25.
  - Call Reference - identifies the B channel call to which this message refers.
  - Message Type - identifies which message is being sent.

Instructor Demo: DIRECTED.SYC, frame 3 is phone number, 100 is 64k call setup.

Q.931 Call Setup Message

(Exchanged Between the Network and the User)



- Messages are exchanged between the user and the network.
- These messages are used to convey signaling information between ISDN Layer 3 entities which are referred to as *information elements*.

Q.931 Call Release Messages

(Release Messages are Sent Back to the User)

Release Cause:

"Call was unexpectedly disconnected!"
(The receiving party pulled the phone plug!)

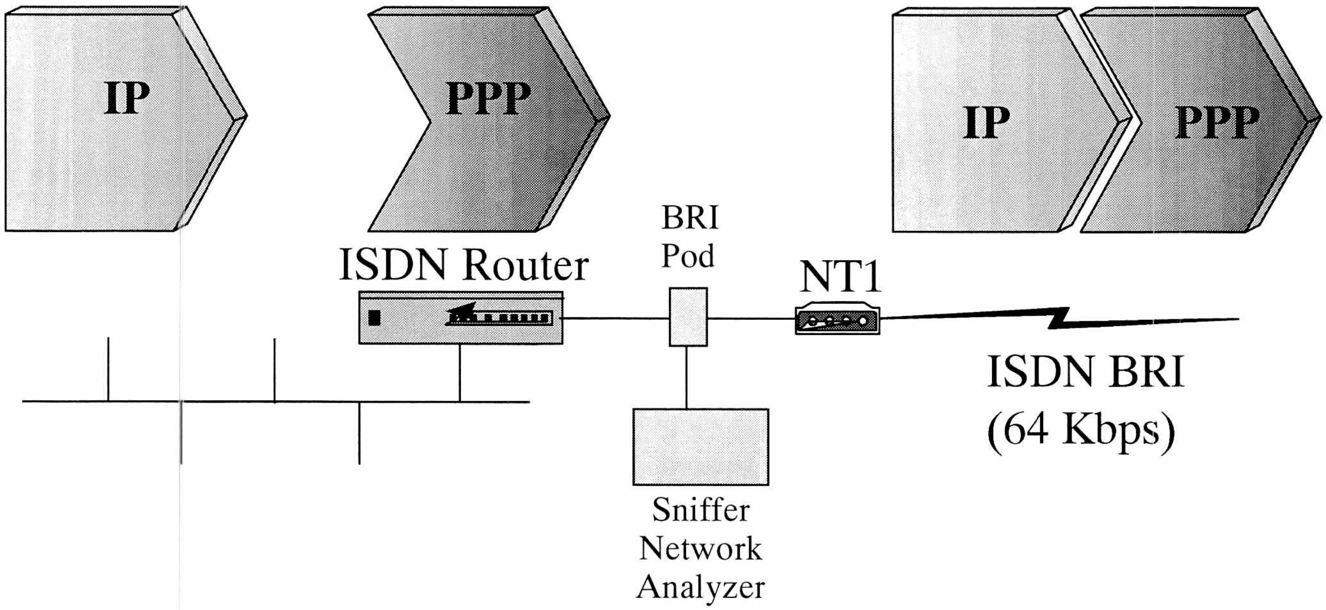
- When the call is terminated the network will let the calling party know that the connection has been released.
- Calls can be disconnected or "dropped" for a number of different reasons (e.g. the remote router drops calls over 10 minutes in length, loss of power on the ISDN line, or loss of call signaling information).
- Within the DISCONNECT and RELEASE messages there is a *cause* field that "explains" the release. If the call was terminated normally the release cause will show a "NORMAL RELEASE".
- However, if the call was terminated abnormally, the release cause will show an error code.
- This is one of the ways to troubleshoot abnormal call releases. Taking a look at the D channel signaling, users can follow the call establishment events and see how the call was terminated. Focusing on the cause codes can reveal the origin of the connection problem.

DEMO: DMS100-D.SYC for release messages

Key Points to Remember!

- Q.931(I.450, I.451) is the protocol that controls the entire channel connections (e.g. call setups).
- Q.931 relies on LAP-D to carry information messages to and from the ISDN network.
- Over 70 Q.931 information messages are defined.
  - e.g. Setup, Call Connected, Disconnect, Release

Internetworking LANs over ISDN



SNIFFER® UNIVERSITY

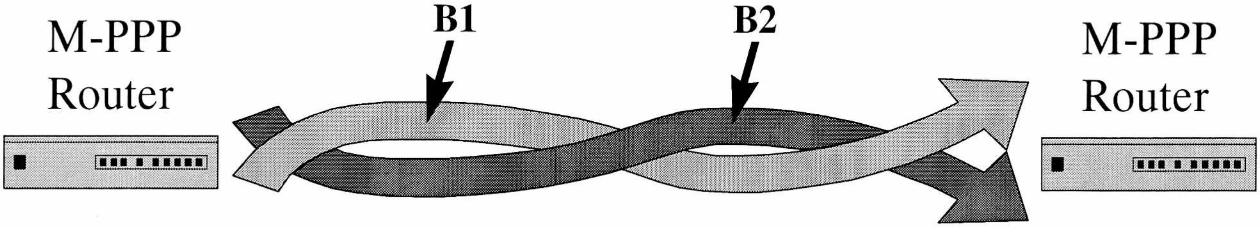
ISDN Concepts 9 - 44

Internetwork Analysis and Troubleshooting, 10/96, Rev. 5.0

Network General

- Remote access routers are the main products used for connecting LAN's over ISDN. The ISDN standards are gradually taking shape, but there is still some work to be done on standards concerning interoperability between products.
- The point-to-point protocol (PPP) establishes a standard way for routers to set up a session, monitor the link, and terminate the session.
- PPP is based on an earlier point-to-point protocol, SLIP. PPP is defined in 10 different RFC's and vendors are allowed to choose which features and functions they will support. Examples of PPP RFCs are RFC1376 PPP DECnet Phase IV, RFC 1378 PPP AppleTalk, and RFC 1618 PPP over ISDN.
- The problem is that vendors can support only one RFC or even a subset of a single RFC and still claim that their products are PPP compliant. Small remote router companies specializing in ISDN, are still having difficulties making their products work with bigger vendors.
- If an access router's PPP feature set does not match that of the central site router, the two may not work together. The only sure way to know if routers will operate together is to try them out. When the two routers attempt to link up using PPP, each announces to the other what feature it supports. Obviously if the two routers have nothing in common, then there is no way to communicate.

ISDN Customer Premise Equipment Multilink-PPP (M-PPP)



- Enhanced version of PPP.
- Defined as a standard (RFC 1717).
- Router establishes one or two B channel calls dynamically as needed for bandwidth. The router also encodes so the frames are sequenced correctly on each B channel.
- Simultaneously sends sequenced PPP frames over two B channels.
- M-PPP Provides 128 Kbps data throughput as needed for LAN-to-LAN connections.

SNIFFER® UNIVERSITY

ISDN Concepts 9 - 45
Internetwork Analysis and Troubleshooting, 10/96, Rev. 5.0

Network General

- New ISDN routers that are on the market are supporting an enhanced PPP protocol implementation called Multilink-PPP, or M-PPP.
- M-PPP is based on an LCP option negotiation that permits a system to indicate to its peer that it is capable of combining multiple logical links into a "bundle".
- M-PPP is negotiated during the initial LCP option negotiation. A system indicates to it's peer that it is willing to do M-PPP by sending the multilink option as part of the initial LCP option negotiation.
- Although M-PPP has been submitted for comments to IETF (Internet Engineering Task Force) only a limited number of router vendors have implemented M-PPP. This method of combining of B channels via software will become the de-facto standard for ISDN routers.

M-PPP Benefits

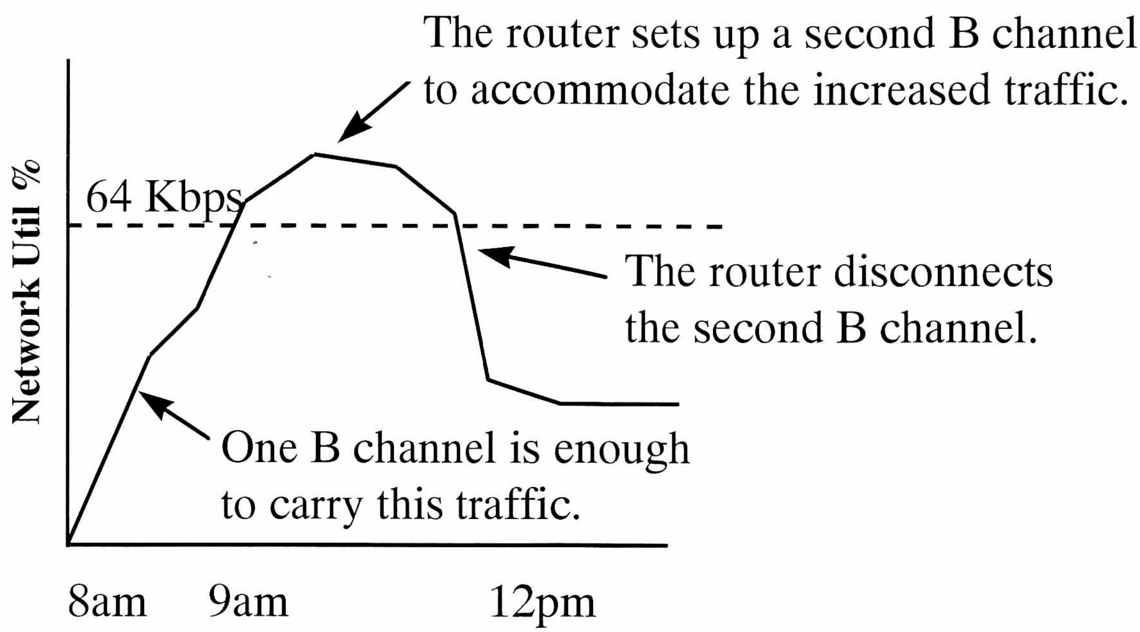
- It's a multi-vendor accepted standard.
- Uses two B channels to move twice as much data as needed.
- Encoded as software means easy upgrades.
- Will soon be implemented for PRI routers.
- Bandwidth on demand.

- With the advent of the M-PPP standard, ISDN routers vendors are working towards developing a compatible routing protocol so that various routers implementing M-PPP can work together. Router vendors will of course provide their own M-PPP implementations in addition to the standard M-PPP.
- Because M-PPP works on the principle of combining multiple B channels to create a larger "pipe", it fits with ISDN's dial-up nature. Users can now move twice as much data over a BRI circuit just by dialing up a second B channel call, instead of adding a dedicated circuit.
- M-PPP is software defined which means that routers that have ISDN interfaces can be upgraded to support M-PPP in the future, provided the vendor has an upgrade path.
- The M-PPP specification does not limit the scope of implementation on BRI circuit only. In fact, M-PPP can accommodate larger bandwidth increments provided the router vendor supports it. There are very few PRI routers that support M-PPP today. As ISDN PRI tariffs begin to come down, more users will begin to adopt PRI. This will drive more PRI router vendors to support M-PPP in the near future.

ISDN Customer Premise Equipment

ISDN Routers

Bandwidth on Demand!



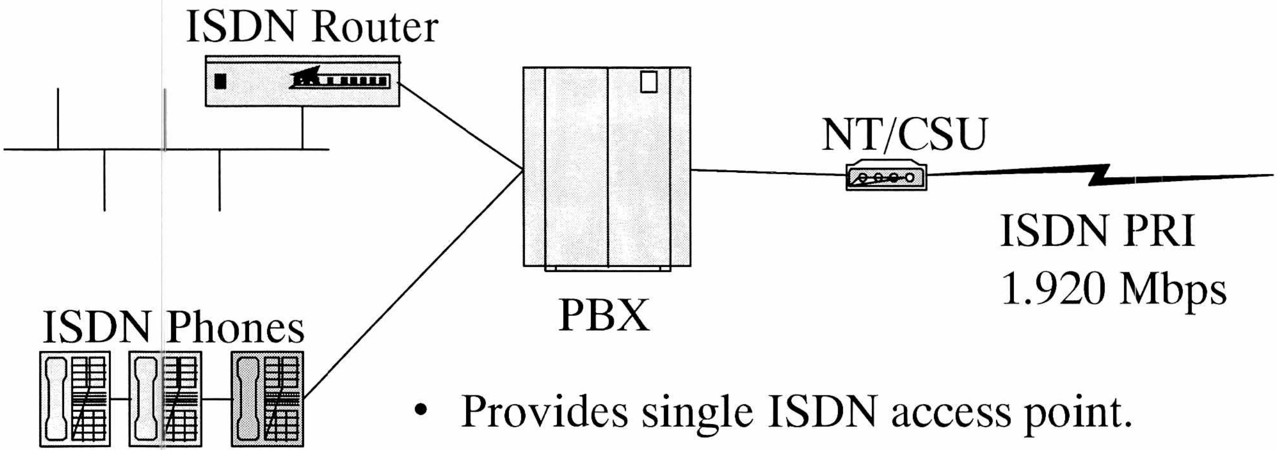
Router Throughput

- ISDN routers take advantage of the unique dial-up bandwidth attribute that ISDN provides.
- The router can be programmed to call up another B channel if the network utilization begins to rise above a pre-defined threshold. When this occurs routers can increase bandwidth by calling up 64Kbps increments.
- Likewise when the utilization falls below the threshold, the B channel is terminated.
- ISDN routers with dial-up bandwidth capability are cost effective alternatives to 64Kbps leased line connections or high-speed analog modem connections.
- With ISDN, the circuit is digital. The connection setup time is much faster than a high-speed analog modem. And because of the dial-up nature of ISDN, the user only pays for the connected calls, leased line users pay a flat rate month regardless if the line is used or not.
- The user needs to make sure utilization thresholds are set properly on the router. Some routers do incur some time when calling up a second B channel. If the router doesn't execute the second B channel call quick enough, frames may be lost due to high-utilization.
- Typically, an ISDN call setup is less than a second, in some countries the time for setup maybe longer.
- Typically, the call teardown time is 30 seconds, so you may need to change the timer when using RFC 1582 (Spider RFC).

ISDN Customer Premise Equipment

The PBX Connection

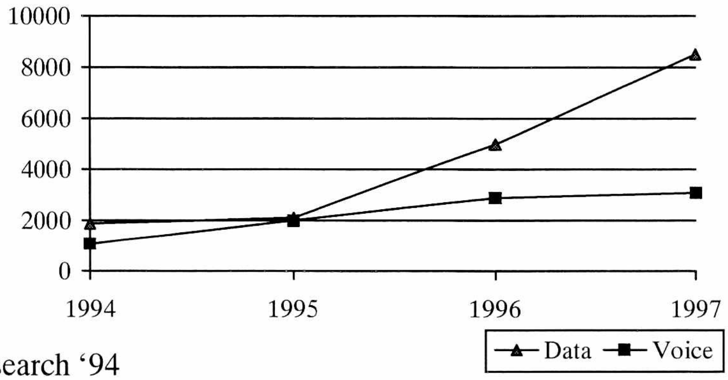
"Voice and Data Hub"



- Provides single ISDN access point.
- Data-ports provide hub functionality.
- User programmable to allocate fixed. or scaleable bandwidth.

- The majority of ISDN circuits installed in Europe will be connected to a PBX (public branch exchange). This is not because voice is a major application over ISDN, but rather the PBX provides rudimentary ISDN hub functions.
- For 2.048 Mbps of bandwidth, only 1.920 Mbps is usable for data.

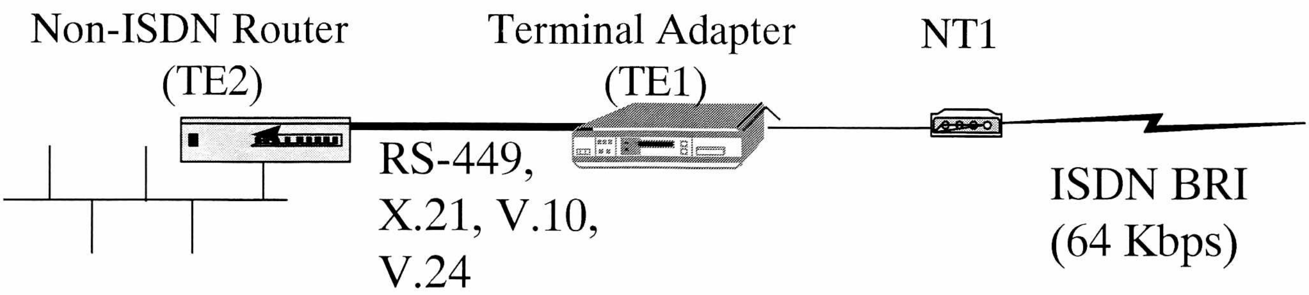
European Voice vs. Data over ISDN



- Source: EuroLAN Research '94
- The difference between voice and data channel usage begins to level out at the end of 1995. This due to the increase, from 1994, in data usage over ISDN in all European countries. The split then widens between 1995 and 1996 as demand for data solutions for remote access and back-up is met by larger coverage and lower tariffs. By 1997, nearly 70% of ISDN channels will used for data.

ISDN Customer Premise Equipment
Terminal Adapter

"The ISDN Converter"



- Connects non-ISDN equipment to ISDN.
- Allows data rates below 64 Kbps to be transferred over ISDN.
- Supports voice, data, fax and video traffic.

- The main purpose of a terminal adapter (TA) is to interface a non-ISDN device to the ISDN circuit.
- It also allows slower traffic, below 64Kbps, to be multiplexed on a 64Kbs B channel.
- The TA manages the ISDN call setup and acts like a modem to the non-ISDN device.
- The TA is often the only way to preserve the customer's original equipment investment when moving to ISDN. If there are routers already installed that are not ISDN-ready, the easiest way to make the existing equipment work with ISDN is a TA.
- When analyzing data in a TA environment, there are two access points to connect the Sniffer Internetwork Analyzer. The first access point is at the S/T interface, or between the TA and the NT1. The second access point is at the R interface, or between the TA and the router (RS-449, X.21, V.10, or V.24) side. The latter access point does not require an ISDN interface, but rather the traditional balanced interface cables.

Key Points to Remember!

- PPP is the most common router protocol used over B channel connections.
- M-PPP is becoming the de-facto standard for the dynamic routing of data over one or more B channels.
- Bridges and routers are often connected to a PBX that is connected to ISDN.

Summary

- User-network interfaces are composed of functional groups and reference points.
- Circuit and packet switching is available.
- Multilink PPP allows sequenced frames over more than one (up to 30) B channels simultaneously.
- Primary Rate Interfaces have 30 B channels (EISDN) or 23 B channels (NISDN) and 1 D channel on Point-to-Point Connections only.
- Basic Rate Interfaces use 2B and 1 D channel and can be Point-to-Point or Multipoint connections.
- ISDN uses B channels in many configurations including H channels to transport data.
- The D Channel sets up, maintains and releases the connections using standard protocols.

Using the Sniffer Internetwork Analyzer with ISDN Analysis

SNIFFER® UNIVERSITY

Using the ISDN Sniffer 10 - 1
Internetwork Analysis and Troubleshooting, 10/96 Rev 5.0

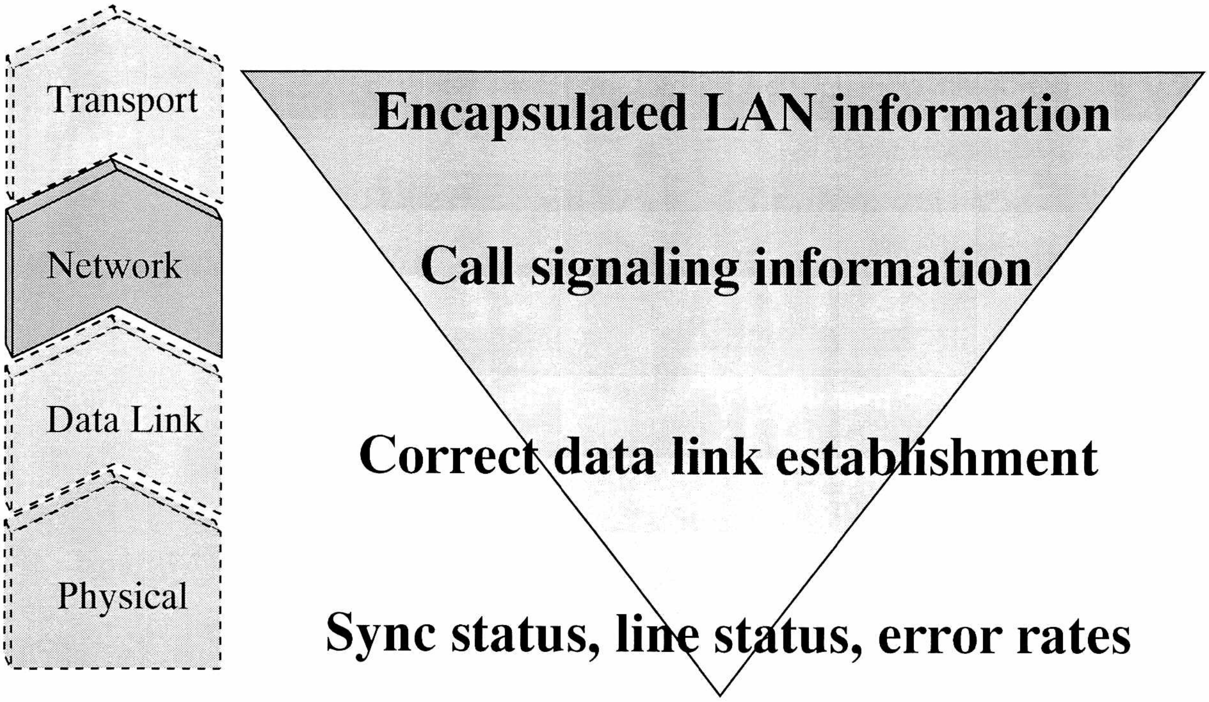
Network General

Objectives

On completion of the section you will be able to:

- Use the features of ISDN support module for the SIA Analyzer.
- Insert the SIA into a Primary Rate ISDN circuit.
- Insert the SIA into a Basic Rate ISDN Circuit.
- Use the Analyzer to troubleshoot common problems in an ISDN network.

Sniffer Internetwork Analyzer
ISDN Analysis Layers



SNIFFER® UNIVERSITY

Using the ISDN Sniffer 10 - 3
Internetwork Analysis and Troubleshooting, 10/96 Rev 5.0

Network General

- The SIA provides detailed protocol analysis and real-time statistics at Layers 2 (LAP-D) and Layer 3 (Q.931, EuroISDN, etc.) and extends the visibility beyond Layer 3 by providing detailed protocol analysis at Layer 4 and above.
- True internetwork application are made up LAN-to-LAN conversations over wide area facilities, therefor LAN protocols transmitted over the WAN communications facilities.

Sniffer Shows Active and Inactive B Channel Connections

- On a PRI, the D channel is always setting up and disconnecting B channels.
- You need to see the sequence of events for **all** B channel connections.

B Channel 12:
- Setup
- Call Proceeding
- Connected
- Info Transfer
- Disconnect
- Release Complete

B Channel 18:
- Setup
- Call Proceeding
- Connected
- Facility Reject

B Channel 23:
- Setup
- Call Proceeding
- Disconnect
- Release Abnormal
- Release Cause: No Answer!

SNIFFER® UNIVERSITY

Using the ISDN Sniffer 10 - 4

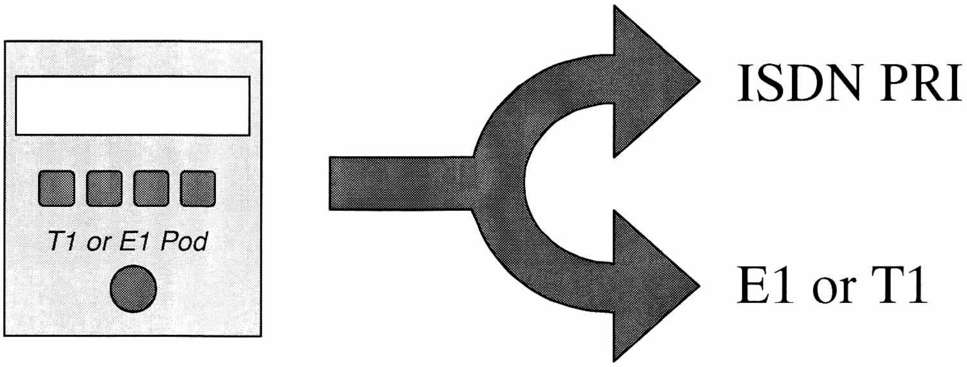
Internetwork Analysis and Troubleshooting, 10/96 Rev 5.0

Network General

- The existing E1-Pod that will be used to monitor the PRI circuit, will **not** be able to automatically re-configure itself to monitor a selected B channel.
- This means when on a PRI circuit, the first thing analyzed should be the D channel. The SIA will keep track of all the B channel call setups and disconnects, providing the user with the B channel number (e.g. B12, B25, B27, etc.). The user can manually configure the E1-Pod to the appropriate 64Kbps channel to see a B channel conversation.

Existing T-1 and E1-Pods are Used to Connect to a *PRI*

- The Pods can also be used for fractional **or** full T1 or E1 circuits.



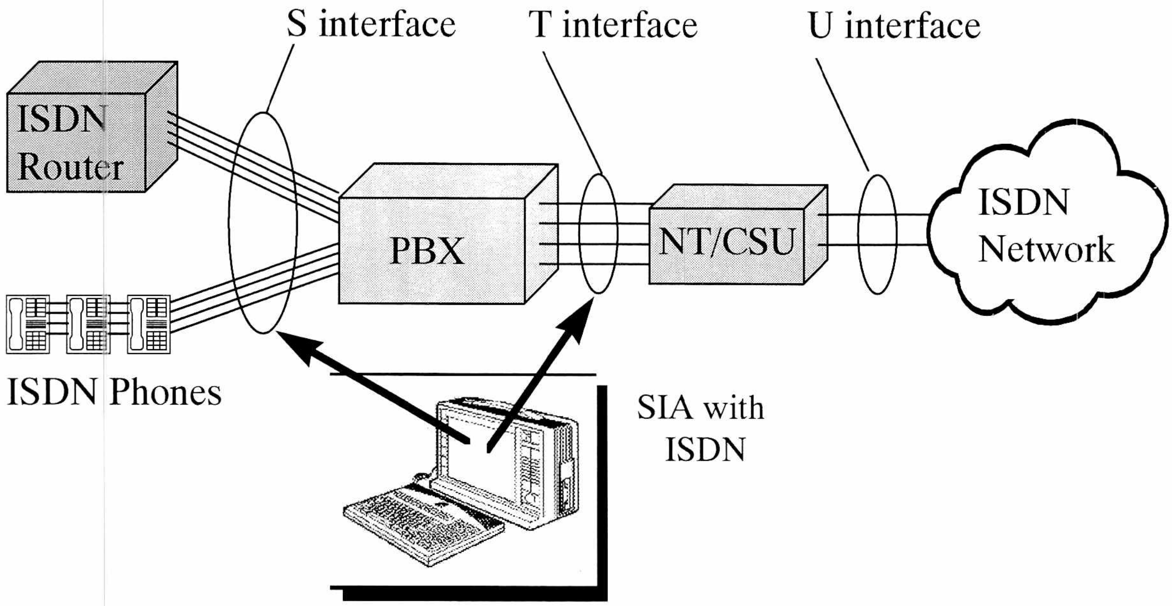
SNIFFER® UNIVERSITY

Using the ISDN Sniffer 10 - 5
Internetwork Analysis and Troubleshooting, 10/96 Rev 5.0

Network General

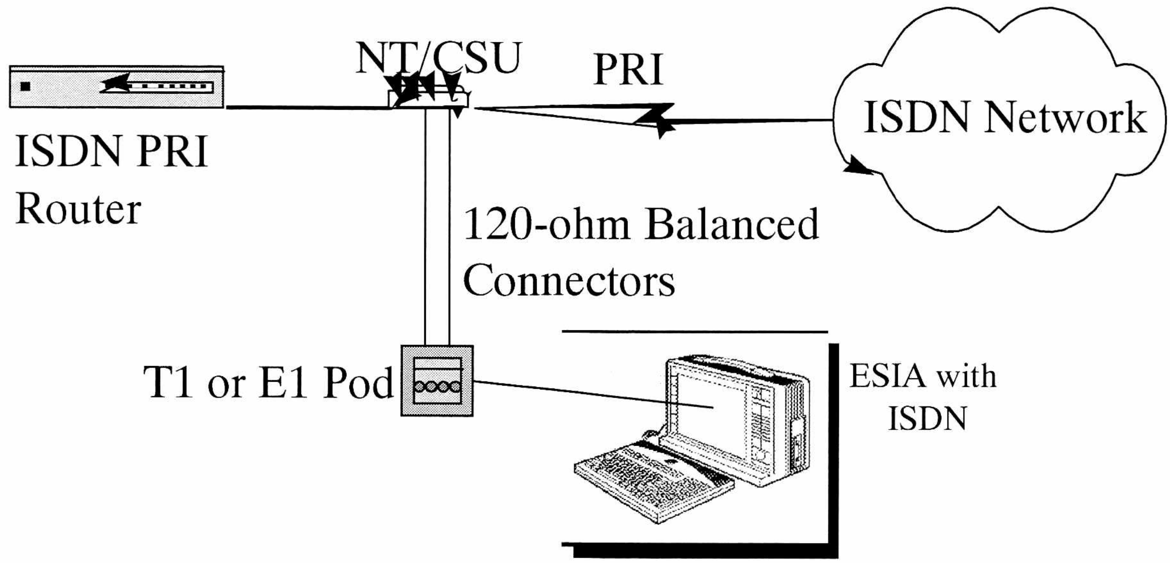
The same E1-Pod used for ISDN PRI access.

Connecting to a *PRI* Circuit



- A common primary rate interface (PRI) connection will most likely terminate at a customer's PBX (or TE2). There is no NT1, as the NT1 is specifically defined for BRI. Instead, the PTT will provide a network termination (NT) in the form of a CSU or a combination CSU/DSU (channel service unit / data service unit).
- PRI is really ISDN over an E1 circuit. Therefore the customer's configuration for a PRI will be nearly identical to a traditional E1 installation.
- The NT in a PRI configuration performs similar functions as the NT1 in a BRI configuration. It terminates the line from the PTT, and prepares the circuit for data transmission by providing synchronization, and framing.
- The PBX acts as an "ISDN hub". From the PBX, several connections can be made to both ISDN-ready and non-ISDN routers, digital phones, and digital fax machines.
- Typically the Sniffer Internetwork Analyzer can connect at either the S interface between the ISDN router and the digital PBX, or at the T interface between the digital PBX and the NT.
- In order to access the ISDN data at the T interface, the E1-Pod is required.

Sniffer Internetwork Analyzer
PRI Interface



SNIFFER® UNIVERSITY

Using the ISDN Sniffer 10 - 7
Internetwork Analysis and Troubleshooting, 10/96 Rev 5.0

Network General

- The E1-Pod's placement is usually at the customer's NT or CSU.
- The customer must manually configure the E1-Pod's framing timeslot (channel) prior to monitoring.

ISDN Sniffer
Basic Rate Features

- Simultaneous 2 B channels and D channel monitoring with real-time statistics
- Real-time D channel protocol monitoring
- Internetwork protocol frame counts on B channels
- 64Kbps and 56Kbps B channel support
- "Simple-Configuration" pod design

It supports the following ISDN switch protocols:

Generic Q.931

EuroISDN (ETSI)

AT&T Custom (ATT 5ESS)

NT DMS-100

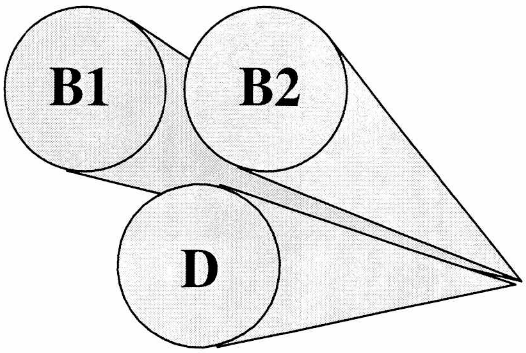
NTT

National ISDN-1 and 2

Australia

Monitoring all Three Channels on a *BRI* -- Simultaneously

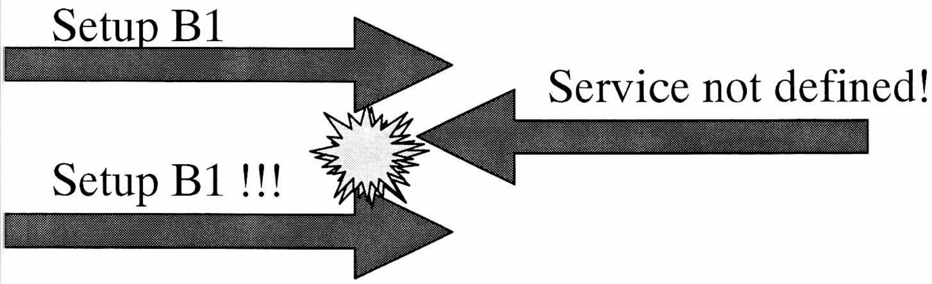
- "Bursty" internetwork applications require two B channels to move data.
- In order to analyze the traffic we need to see both B channels in action!



- In addition, the SIA shows the D channel in action while the two B channels are connected. This is a useful feature when trying to pinpoint connection problems.
- The SIA provides real-time statistics for the two B channels and for the call signaling information on the D channel.

Real-time D Channel Protocol Monitoring

- 70% of the ISDN connection problems occur in the signaling messages on the D-channel.
- In order to effectively troubleshoot ISDN connections you **need** to see the D channel in action!



- The SIA provides a "history" of the D channel call signaling messages so the user can scroll through and study the events.
- A common problem that customers often find on an ISDN BRI or PRI circuit is that the service they ordered is not what is installed.
- For example, a company attempts to setup a 64Kbs, 8kHz structured, unrestricted data call on a B channel, but the network responds back indicating that the service is not defined.
- The problem is that the subscriber is setup up for 64Kbs, 8kHz structured, <u>speech</u> and not for an unrestricted connection. Asking for a specific service to be invoked by the network when the user is not setup for it will result in an error.
- ISDN service ordering is still not consistent throughout all the European PTTs. In fact, ISDN installations are still entered in by operators through paper service orders.
- Without analyzing these Layer 3 messages to and from the network, the customer will not be able to identify the real-problem.

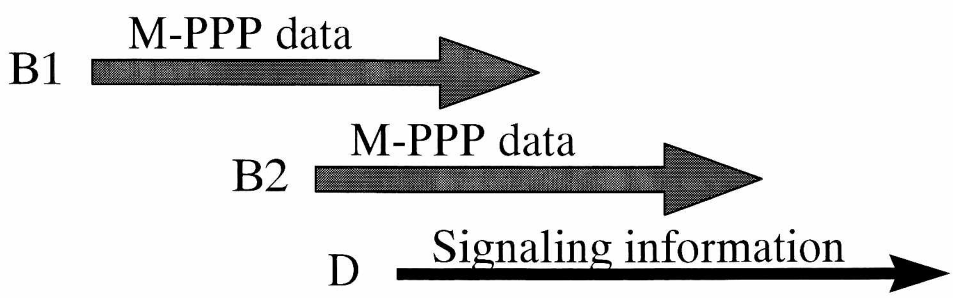
Internetwork Protocol Frame Counts on B Channels

- Provides an indication of the type of LAN protocol traveling over the B channels.
- When setting up an ISDN router for the **first** time you can make sure the device is transmitting correct frame formats.

- The internetwork protocol frame counts are, in a way, a real-time protocol decode on the B channels.
- In order for the SIA to count the frames of a particular protocol type, the analyzer needs to understand or "decode" the frame in real-time.
- Though the SIA doesn't show the full detail of the protocol in real-time, the frame counts provide a low-level protocol usage gauge.

MultiLink-PPP Support

- M-PPP has become the de-facto standard for transmitting routed data over **two** B channels.
- When troubleshooting a M-PPP router connection problem you need to see **both** B channels, **plus** the D channel at the same time!

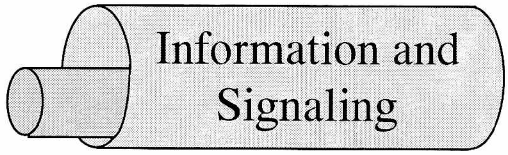


The M-PPP protocol is relatively new in the industry. Network General continues its leadership in technology by providing a protocol decode for the Multilink-PPP RFC 1717 standard.

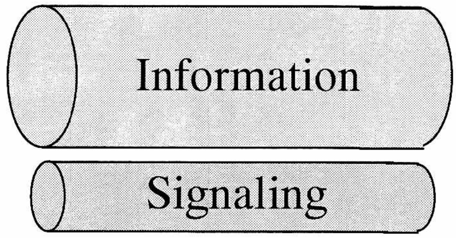
B Channel Support
56Kbps and 64Kbps

- European and Japan ISDN B channels are 64 Kbps.
- U.S. ISDN B channels are 56 and 64 Kbps.

U.S.
(in-band signaling)



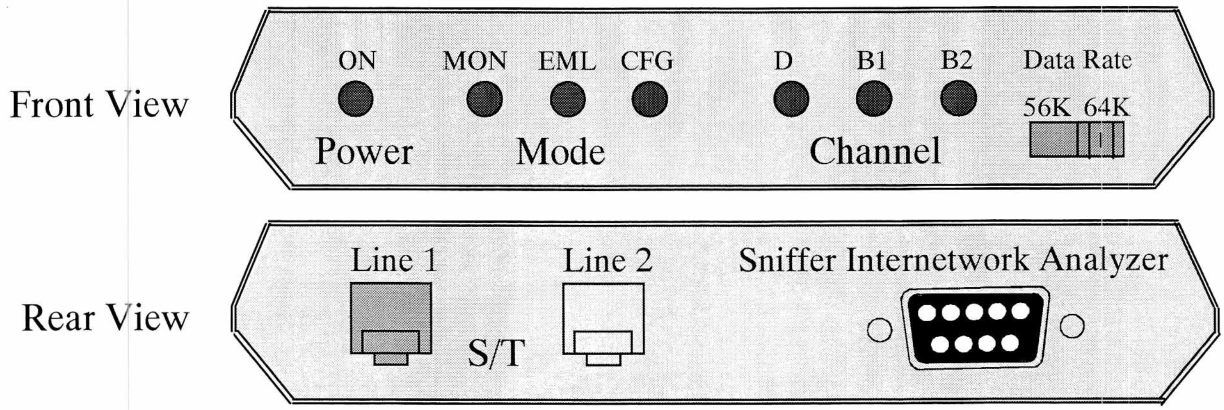
Europe
(out-of-band signaling)



- In the US, where ISDN service is not available, the carrier will extend ISDN via a service call BRITE or Basic Rate Interface Terminal Emulation. Because BRITE is emulating a BRI circuit, the call signaling information occupies part of the B channel bandwidth.
- The ISDN interface pod will have support for these two types of signaling methods.

"Simple-Configuration" Pod Design

- All **BRI** channels are monitored automatically.
- Dual RJ-45 jacks enables quick installation.



The ISDN BRI interface pod is designed to be "plug and play".

Once the pod is connected to the ISDN circuit it will automatically begin monitoring the two B channels and the D channel.

Front View of the Pod:

MON - monitoring, will light when the mode is in monitor mode (normal traffic mode).

EML - emulation, not supported in the first release.

CFG - configuration, will light when the SIA is downloading configuration information to the pod (e.g. 56K or 65K monitor).

D - On when D channel is being monitored (always on).

B1, B2 - will light when B1 and B2 channels are being monitored .

Data Rate - a manual switch for either 56K or 64K B channel monitoring. This is for future DSS applications, where the user may need to manually configure the pod.

Back View of the Pod:

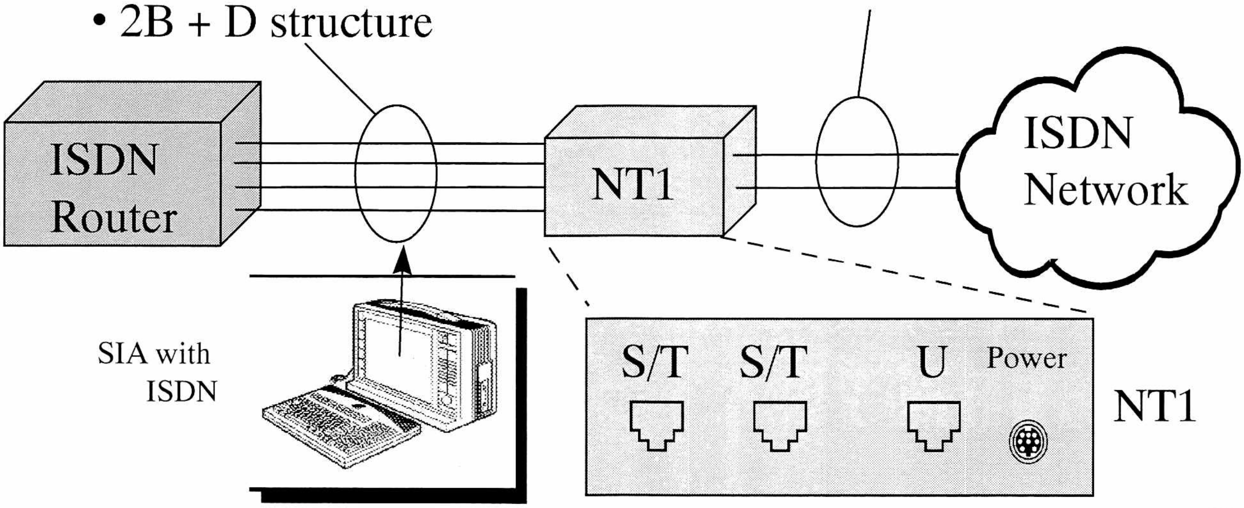
Line 1 / Line 2 - the S/T interface that is used to connect to the ISDN circuit.

SIA Port - a proprietary port used to connect the ISDN BRI interface pod to the Sniffer Internetwork Analyzer. This port is proprietary to Network General only, no other analyzer product can use this port.

Connecting to a BRI Circuit

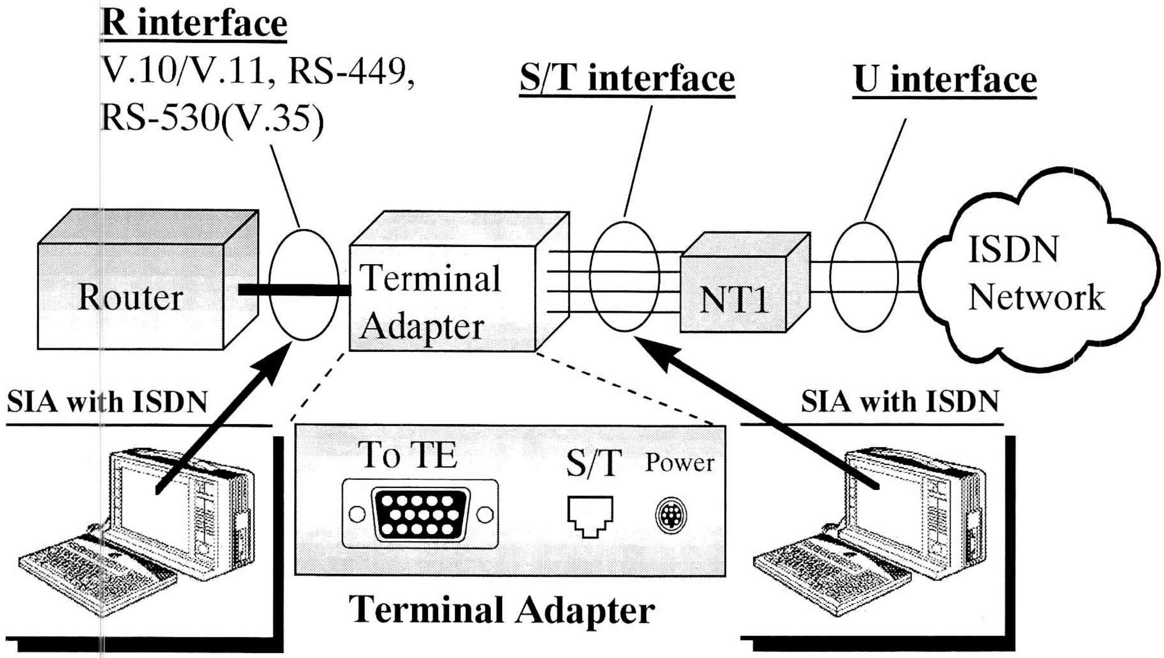
S/T interface
- 8-wire
- RJ-45 (8 pin connector)
- **Power** is added for TE
- 2B + D structure

U interface
- 2-wire
- RJ-11 (2 pin connector)
- No power for TE



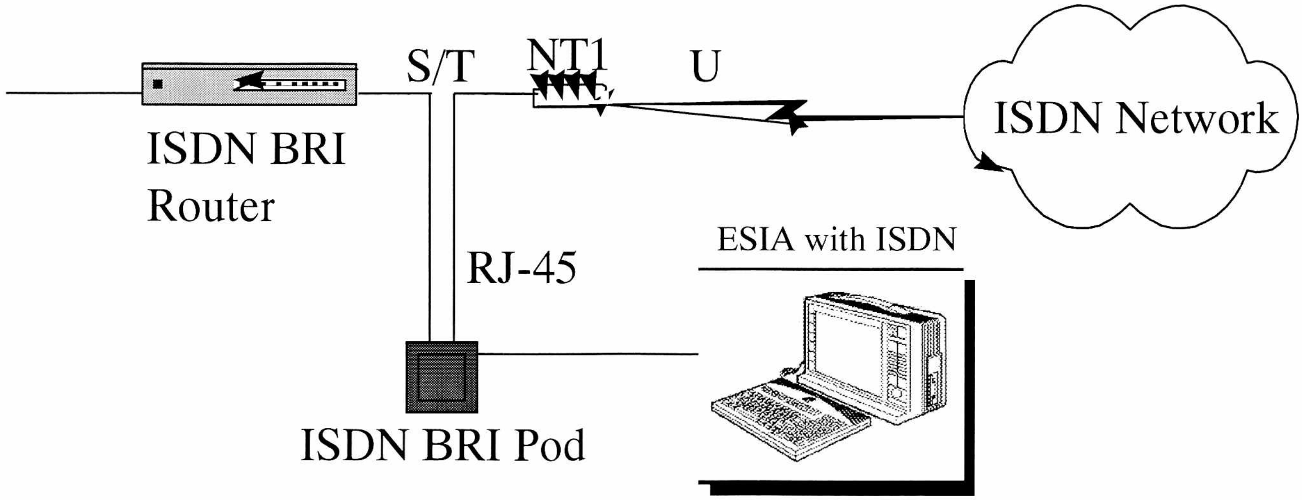
- In a typical BRI installation we see the U reference point, or U interface coming from the network. It is terminated at the NT1, where power is added to the line.
- The PTT only provides the power necessary to generate the signal to the NT1. It is the responsibility of the NT1 to provide the power to the ISDN circuit for the user's connected equipment. That is why there are eight-wires coming from the NT1, two pairs for Receive and Transmit, one pair for power, and one pair for backup power.
- The interface from the NT1 is called the S/T interface. The NT1 will normally have two connectors that the user can plug equipment into.
- The Sniffer Internetwork Analyzer can plug into the NT1 to see the data between the ISDN router (TE1) and the ISDN network.

Connecting to a BRI Circuit



- The main purpose of a terminal adapter (TA) is to interface non-ISDN devices to the ISDN circuit.
- The TA will usually have one ISDN interface to connect to the NT1 and one or more balanced interfaces to connect to non-ISDN equipment.
- When analyzing data in a TA environment, there are two access points to connect the analyzer. The first access point is at the S/T interface, or between the TA and the NT1. The second access point is at the R interface, or between the TA and the router (RS-449, X.21, V.10, or V.24) side. The latter access point does not require an ISDN interface, but rather the traditional balanced interface cables.

Sniffer Internetwork Analyzer
BRI Interface Pod



SNIFFER® UNIVERSITY Using the ISDN Sniffer 10 - 17
Internetwork Analysis and Troubleshooting, 10/96 Rev 5.0

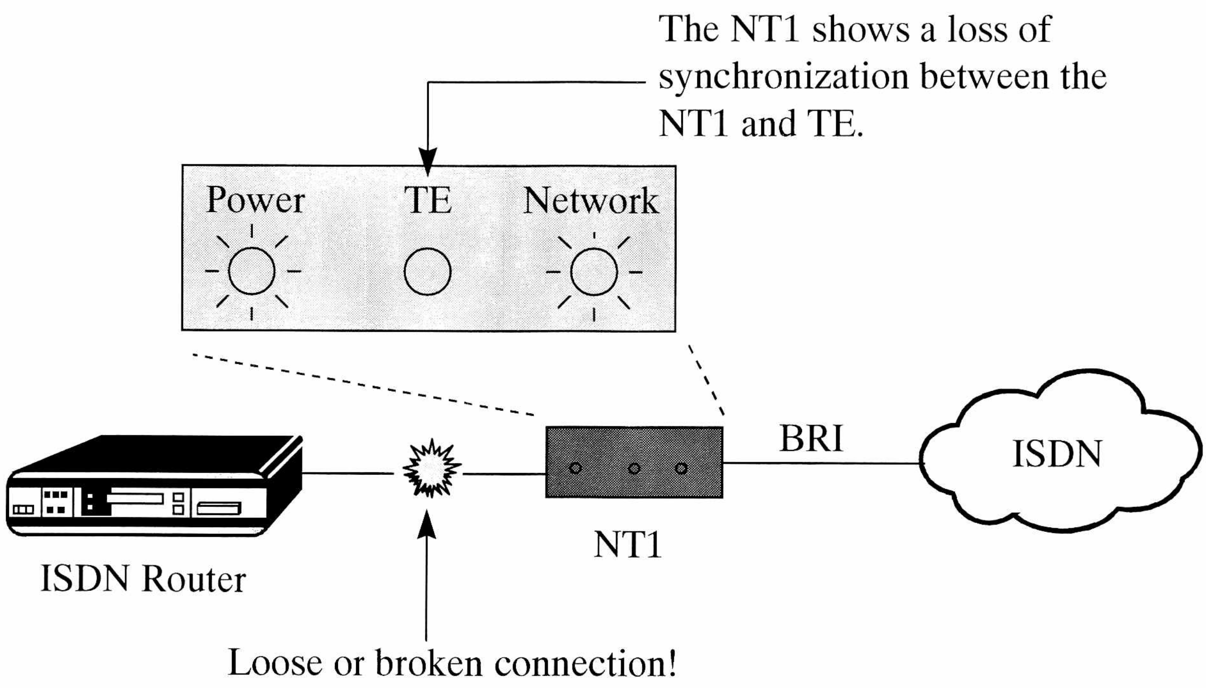
- The ISDN BRI pod connects between the TE and the NT1 at the S/T interface.
- The two RJ-45 jacks on the pod makes connecting between the two devices quick and easy.

Troubleshooting with the ISDN Sniffer Internetwork Analyzer

SNIFFER® UNIVERSITY

Network General

Look first at the NTI



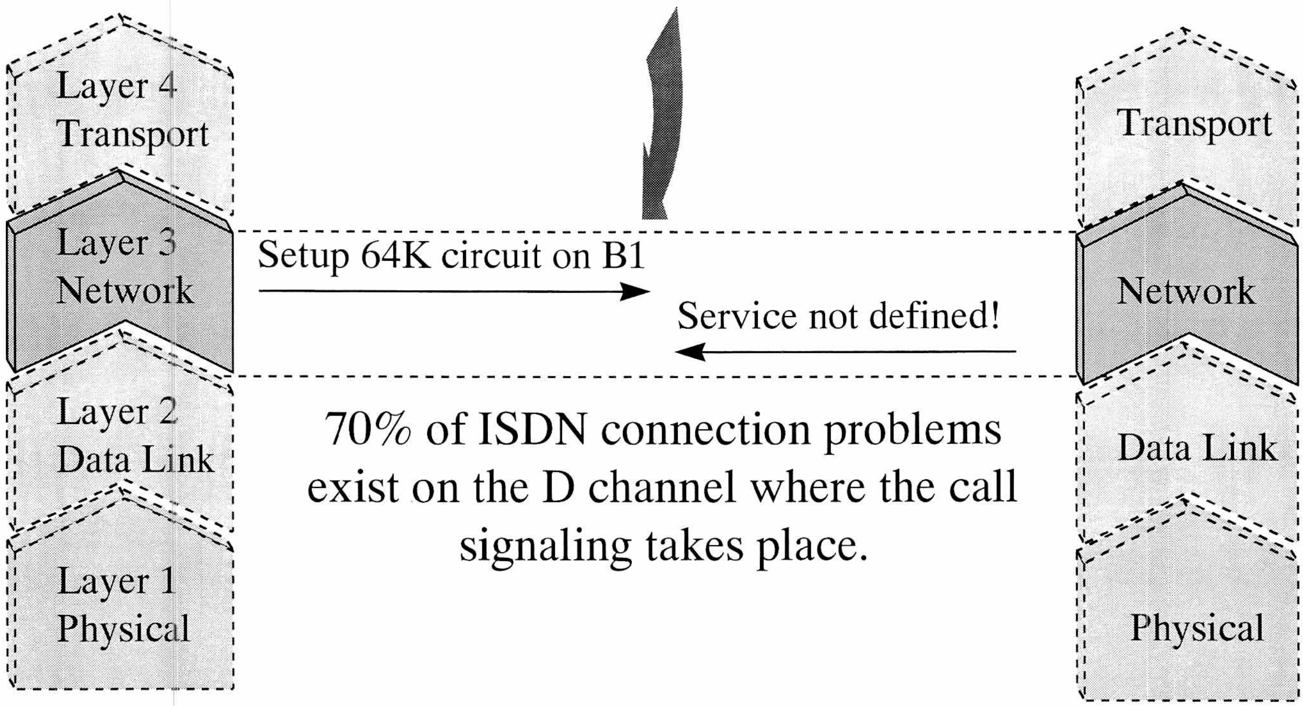
SNIFFER® UNIVERSITY

Using the ISDN Sniffer 10 - 19
Internetwork Analysis and Troubleshooting, 10/96 Rev 5.0

Network General

- When ISDN connection problems occur, normally the first task is to check the connection points and to make sure there are no breaks in the line.
- The NT1 is a good place to start. Since the NT1 is responsible for providing power to the line and to make sure there is synchronization between the TE and the NT1, the NT1 device itself will have status LEDs indicating these functions.
- If there is a loss of synchronization between a connected TE and the NT1, no communication will be able to take place. As soon as the connections are corrected, the TE will begin its establishment procedures with the NT1. The NT1 will then show synchronization from both sides of the ISDN line.

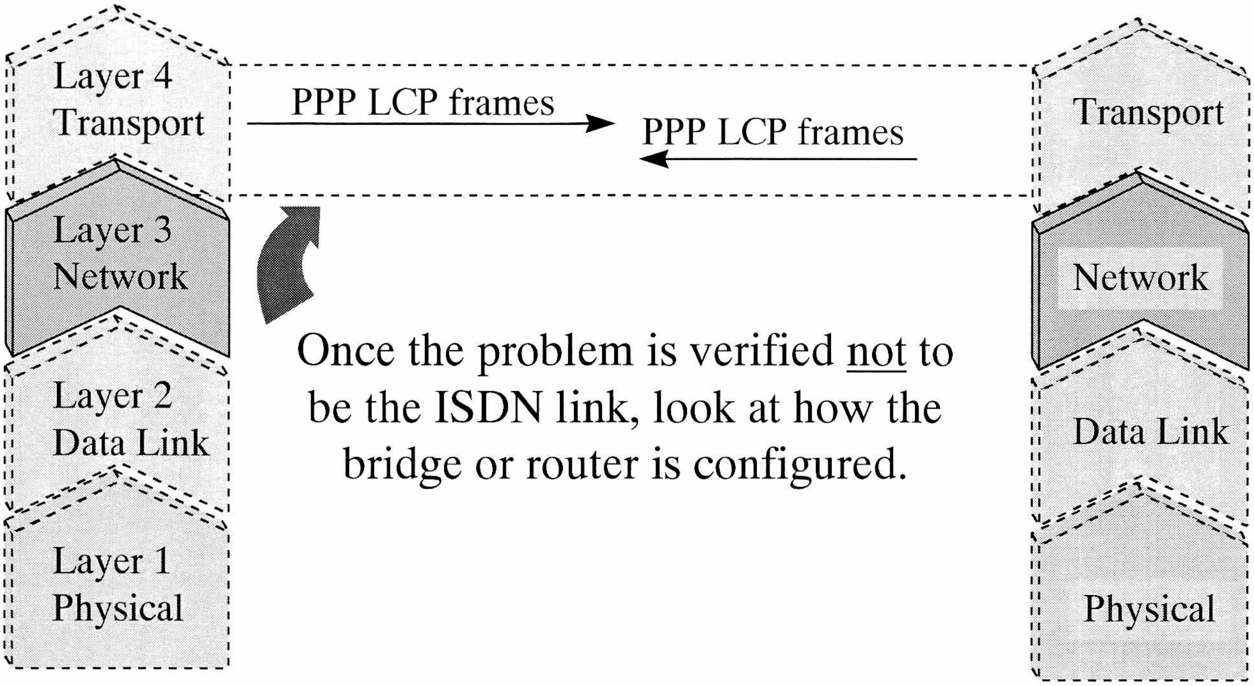
Look Next at the D Channel



70% of ISDN connection problems exist on the D channel where the call signaling takes place.

- If connection problems still exist, after correcting any physical layer problems, the next place to concentrate on is the D channel signaling protocol.
- Look specifically at Layer 3, where the control messages are exchanged between the subscriber and the network.
- 70% of ISDN connection problems exists on the signaling channel, as this is the focal point for all B channel connections.

Check the Bridge or Router



Once the problem is verified not to be the ISDN link, look at how the bridge or router is configured.

Using ISDN Sniffer to Solve Problems

- Solving Problems
  - Disconnect Problems
  - Quality of Service Differences
  - Implementation Incompatibilities
- Optimizing ISDN
  - "Chatty" traffic
  - Unnecessary traffic

Chatty and Unnecessary traffic:

IPX/SPX "Keepalive " Proxy - Novell is a very "chatty" protocol with the file server sending a message to each remote client terminal every five minutes when there is no communications. In a network where the bridge/routers are utilizing ISDN as the transport, these "keepalive" messages can increase the monthly connection charges significantly. Bridge/routers should implement a "spoofing" protocol whereby the bridge/router responds to the "keepalive" messages sent from the file servers without actually bringing up the link.

Demand RIP/SAP - Normal routing protocols cause bridge/routers to communicate with its neighbors to determine which paths are available to transmit data. They normally do this via periodic messages sent throughout the network. Most often, nothing has changed in the network, and the messages do not convey any new information. Bridge/routers should implement either static routing or demand RIP/SAP. Demand RIP/SAP only sends a routing protocol message when there is an change in the topology or new services being advertised. This minimizes ISDN connection charges since only changes are sent across the network. Implement RFC 1582.

More info can be found http://www.acc.com

Setting the Sniffer to Capture from a *PRI* Line

- Connect the pod to the ISDN line.
- Configure the Sniffer to capture in **Classic Mode.**
- Move to the **Options\Line Interface** menu and select **ISDN PRI** and the correct pod.
  - Move to the right and enable the **switch protocol** appropriate for your ISDN switch.
  - If unsure, use the Q.931 generic standard.
- Configure the pod for the characteristics of the line to be monitored.
- Start the capture.

Classic Capture Screen Information

- **D Channel Messages**

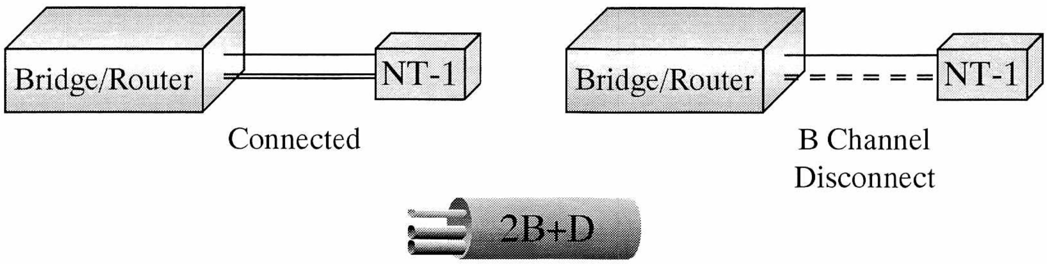
Frames	The number of frames associated with a message.
Ref	The Q.931 call reference number. Following this number allows you to track all transactions relating to a single call.
Chan	The number of the B channel associated with the D channel message.
Q.931	Short description of the Q.931 message (Release+ or Connect).
Phone Number	ISDN phone number associated with the message.
Status	The release cause code information. These are displayed in the Detail window after the data is displayed.
SRC	The source of the message (DTE or DCE).
Duration	The amount of time used by this transaction.

- **Total D channel frame count**
- **The latest Q.931 message type detected**

Possible Problems

Router does not disconnect

- User terminates router connection.
- Router discontinues PPP session.
- D channel does not disconnect the B channels.
- User is billed for connection time during stagnant period.

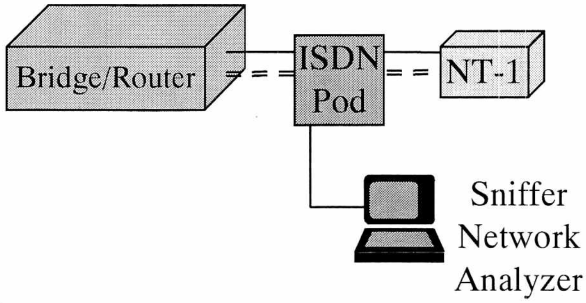


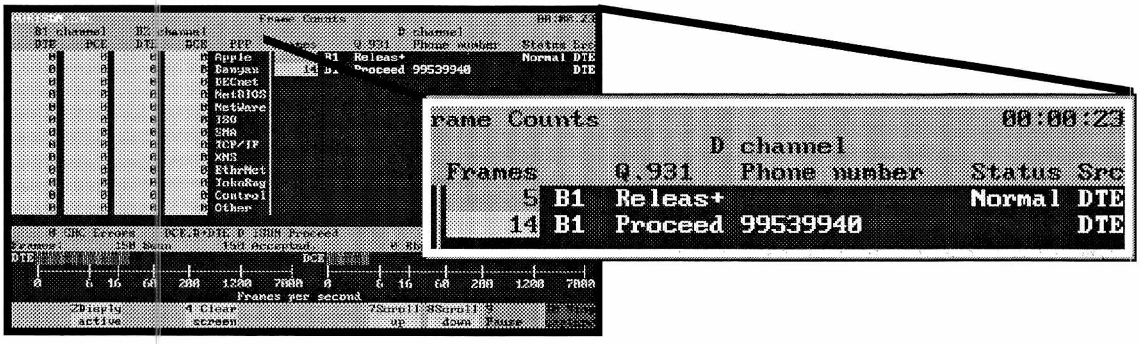
- This problem has been encountered by users of some routing equipment. In this scenario, the router is used to connect two separate LANs. When the LAN connection is completed, the Router disconnects the LAN traffic between the one LAN and the other, but does not "tear down" the ISDN connection. The D channel does not release the B channels.
- As ISDN connections are billed according to the total amount of connection time, this problem can cost organizations a great deal of money.

Possible Problems

Diagnosing Router Disconnect with the Sniffer

- What you will see:
  - Active connection - ISDN & PPP.
  - PPP (on B channel) session close and disconnect.
  - D channel ISDN does not end the connection, despite lack of activity on B channels.

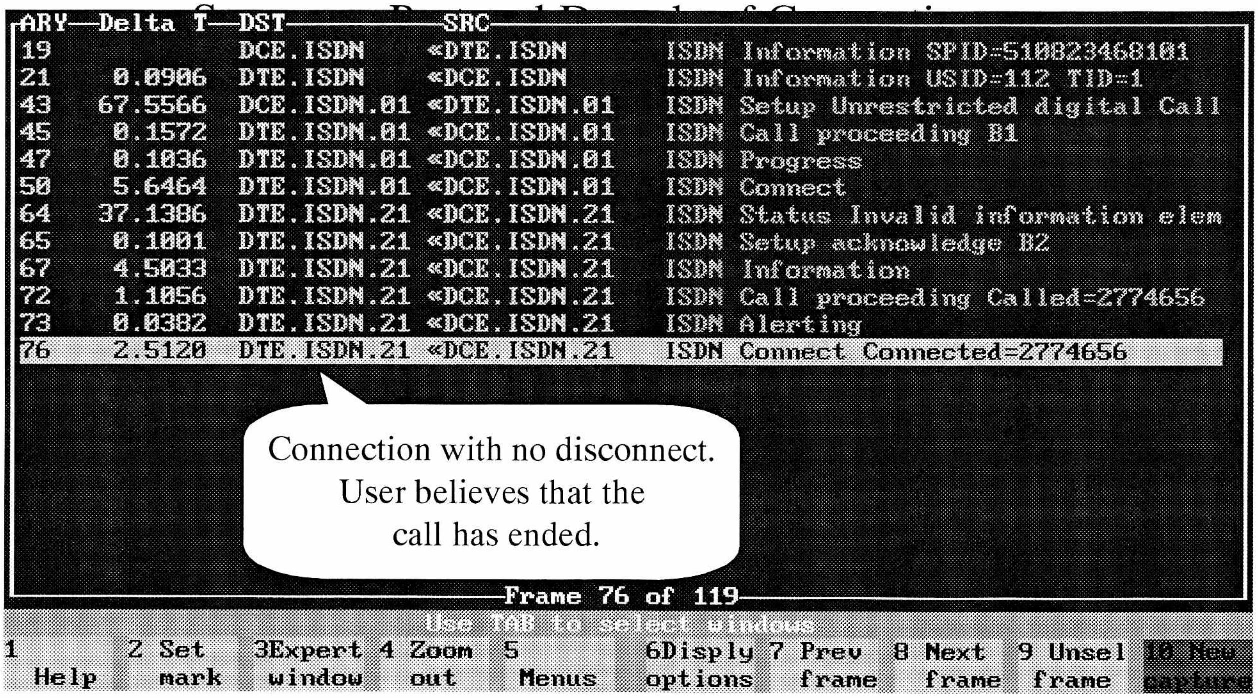




- The ISDN Sniffer shows the status of each ISDN connection. In this screen, disconnected sessions are "blued" out, where active sessions are highlighted in gray.
- This example shows that, at this moment B1 is connected and is exchanging data over "Phone Number" 99539940. There was a previous connection on B1, but is was disconnected.
- If you were using this software to determine whether ISDN was disconnecting the ISDN line after communications were terminated, you could use this screen to show the status of the connection.

Possible Problems

Diagnosing Router Disconnect with the Sniffer



SNIFFER® UNIVERSITY

Using the ISDN Sniffer 10 - 27

Internetwork Analysis and Troubleshooting, 10/96 Rev 5.0

Network General

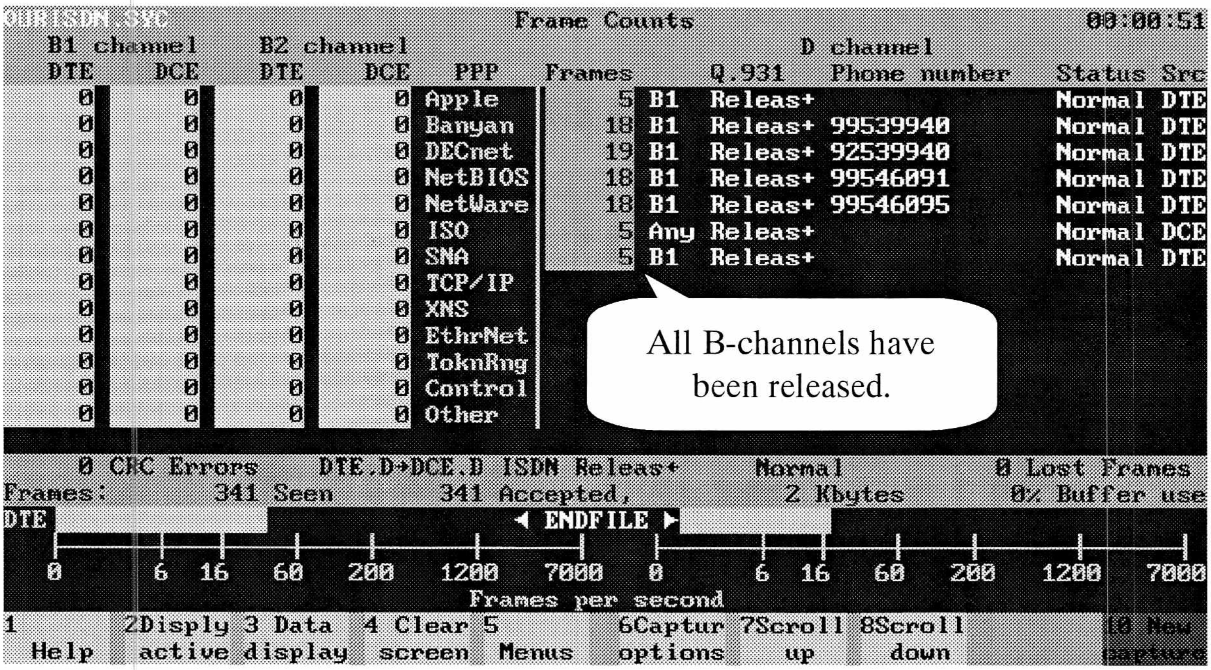
This screen shows the summary line decode of the ISDN connection.

As you can see, the ISDN connection was setup and established, but never disconnected.

Possible Problems

Diagnosing Router Disconnect with the Sniffer

Successful disconnect process



SNIFFER® UNIVERSITY

Using the ISDN Sniffer 10 - 28

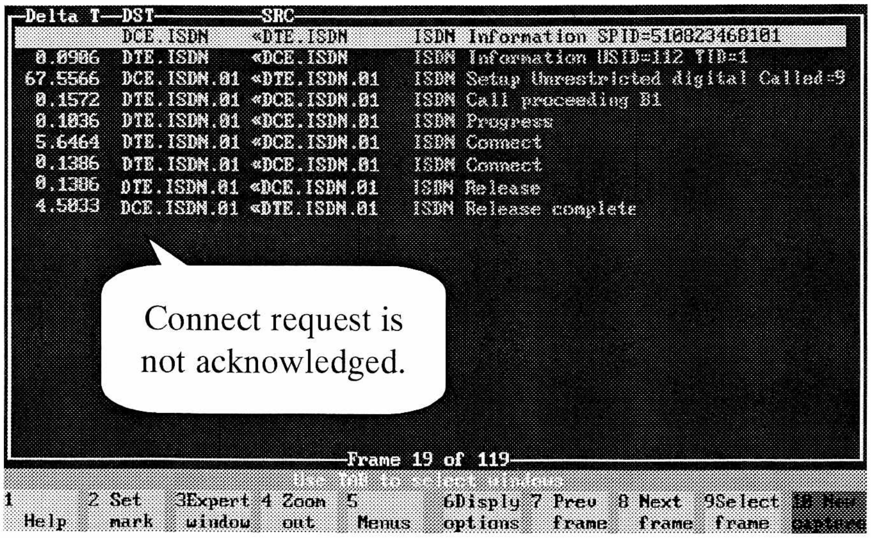
Internetwork Analysis and Troubleshooting, 10/96 Rev 5.0

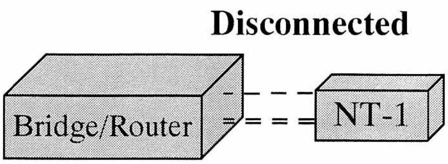
This screen shows a series of healthy connections. Each connection was setup, initiated, data was transferred between the connections, and the call was disconnected.

Possible Problems

Quality of Service (QOS) Differences

- Differences in QOS can lead to time-out errors and disconnects.
- QOS differs from nation to nation.





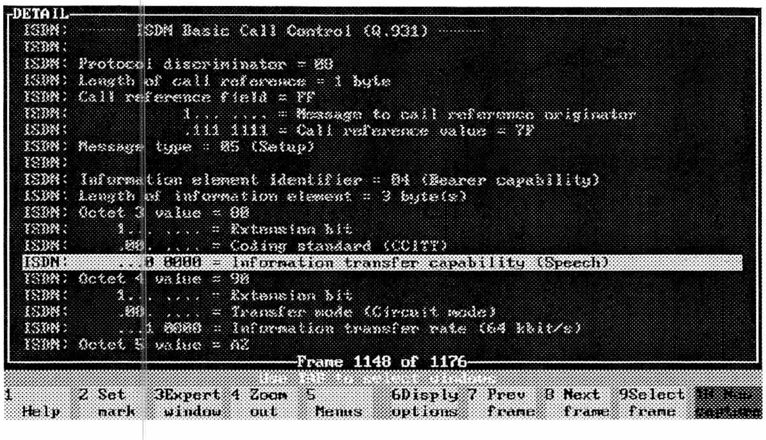
Default Time-out period < Ack time for Connection

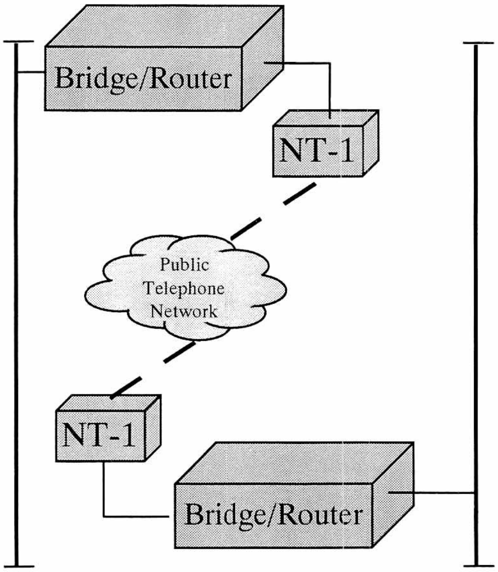
- Each nation that supports ISDN also maintains a different "Quality of Service" (QOS). QOS can effect many things, most notably connection time and latency. There is not QOS standard.
- With ISDN connections, time-out periods can default in the millisecond range. As a result, if equipment defaults to a small time-out period, but the ISDN service provider does not provide the expected QOS, the equipment may fail to connect.
- These time-out periods can be witnessed looking at the summary decode screen. When the user equipment tries to connect to the Telephone office, you will see a connect request. If the ISDN service provider equipment does not respond within the time-out period, you may see a second (or repeated) request(s) and perhaps an eventual disconnect or time-out error. Either way, the equipment may not connect.
- In this example, the QOS setup time property was not consistent with the customer premise equipment.

Possible Problems

Incompatible Vendor Implementations

- Connection problems may occur if ISDN implementations are not similar.





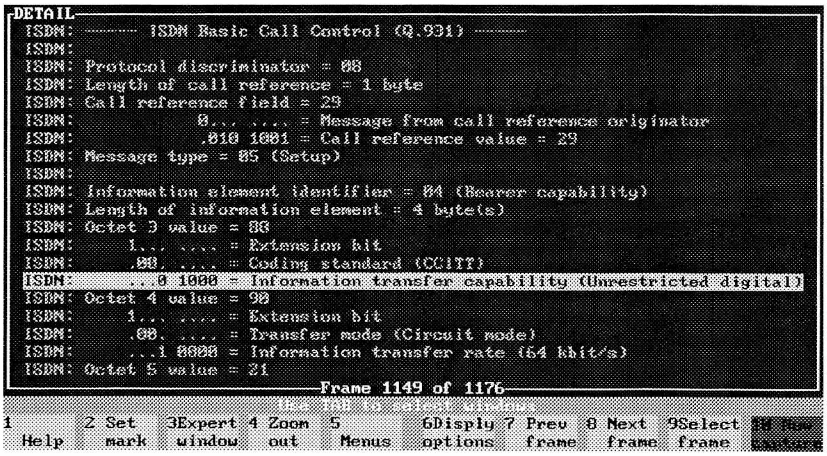
- The type of service must be recognized by the ISDN switch and by the other connected device.

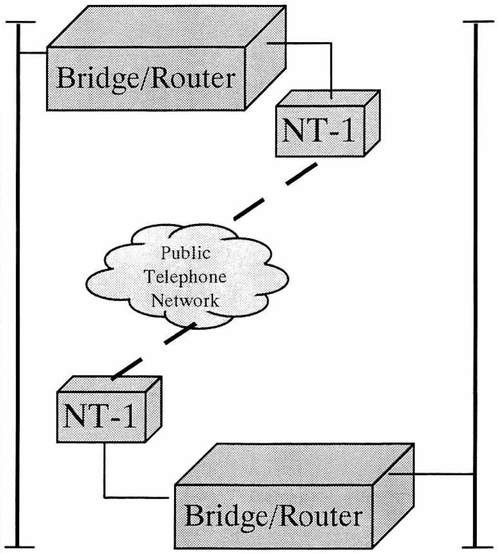
- With ISDN, all parties in the connection must know about the services that are being requested. As such, the device requesting the connection must request a service that the switch and the connection device recognize. If there is any disparity between these devices, the connection will not go through.
- Examining the detail decode can help isolate where such connection disparity is coming from.
- In this packet, one router is trying to connect to a second router using an ISDN connection. The first router requests a service that appears to be a voice connection. The second router is only configured for data connections. As a result, the connection is not established.

Possible Problems

Incompatible Vendor Implementations

- The connection problem may not be ISDN related.
- Check Encapsulated LAN protocol on B channels.





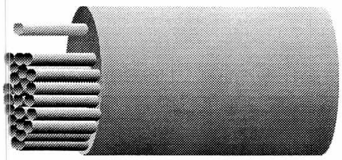
- If the user cannot connect, but the ISDN line appears to connect, make sure the router (PPP) configuration is correct.

- Connection compatibility problems may not be related to ISDN at all.
- In this display, the first router requests an "Unrestricted Digital" service. The second router may recognize and accept the ISDN connection. At this point, a PPP or M-PPP connection may be established.
- If the routers are not setup to communicate correctly using the PPP, M-PPP protocol, or some other connection in the same way, the connection may not be established.
- Because the ISDN Sniffer can decode not only the ISDN and LAPD protocols, but also the encapsulated LAN protocols, these kinds of problems can be resolved quickly and easily also.
- Because the Sniffer can decode the 2B+D, the ISDN connection and the LAN connection can be looked at in chronological order so that relationships can be established.

Optimizing ISDN Networks

Recommendations

- Be careful of "Router Spoofing" techniques
  - Some implementations may create a connection just to transmit RIP packets, SAP packets, or other configuration information.
- Watch LAN traffic over B channels
  - Optimize performance by using "WAN-friendly protocols" (TCP, IPX-Packet Burst, etc).
  - Adjust Time-Out periods to coincide with the QOS setup time and latency of the ISDN service.
  - Filter unneeded LAN traffic from the WAN.



- ISDN connections are usually billed according to the time that they are used. As such, the better the connection is optimized, the less money the organization has to pay for the service.
- Aside from making the connection visibly more efficient, these techniques can help to leverage your ISDN investment.
- A WAN optimized protocol, such as TCP/IP or Packet-Burst NCP, may dramatically improve the performance of your application.
- Decreasing unnecessary traffic on the ISDN connection may also improve the connection speed if congestion is a problem.
- Increasing time-out periods may be an option in circumstances where LAN applications are causing a high rate of retransmissions. This technique could also backfire if the service or server is not responding, increasing the amount of "dead time" on the connection.

ISDN Exercise 1

Objective: To become familiar with Basic Rate ISDN.

Background: An Ethernet LAN is given access to the WWW using an ISDN brouter. The brouter makes use of a facility called "bandwidth on demand".

1. **Load** and display the trace file C:\SYCAP\TC107\DIRECTED.SYC.
2. Press **F5** for Main Menu, **cursor down** to Options, and then **cursor right**. Which Frame Type is being used? Is this appropriate for the type of TE mentioned in the Background above? Which Line Interface is being used? (Note that it should be set to ISDN BRI as this trace was taken using the Basic Rate Interface Pod and not the PRI Pod.)
3. Press **F3** twice to display the data. Press **F6** for Display Options and enable the **Detail** window. Press **F3** to redisplay the data.
4. **Tab** into the Detail window and use the **Home** key to navigate to the top of frame 1. Examine the DLC Header: is this a B-channel in use or a D-channel?

ISDN Exercise 1

Continued

5. Looking at the N(R) values for frames 1 in the Summary window, is the ISDN connection just starting up or is it already started? Which TEI was negotiated between the ISDN network switch and the brouter? Which SAPI?Is this the correct SAPI for this type of action (call control)?

6. In frame 3 we see an ISDN Setup Unrestricted Digital request for a B-channel. From the **Summary** window, what is the telephone number called?

7. Use **F8** to advance to frame 5 which is an ISDN Call Proceeding notice. Looking at the DLC Header, is the B channel or D channel being used to setup the call? From the Summary window, which channel will be setup: B1 or B2?

ISDN Exercise 1

Continued

8. In frame 7 we see the ISDN brouter issue an ISDN Connect to the ISDN network which in turn is acknowledged in frame 9. Looking at frames 11 to 13, does the Combinet ISDN brouter use the D channel to communicate with the ISDN network or does it use the B channel in-band?

9. In frame 62, who is the user connecting to on the World Wide Web? (look in the **Hex** window)

10. By looking at the Detail window of frame 74, determine which TEI and SAPI the ISDN brouter uses to determine the status of the TEIs assigned to it? Are these appropriate for this type of action? From the Summary window decode of frames 75 and 77, which TEIs have been assigned to the brouter?

ISDN Exercise 1

Continued

11. Within the Detail window, if you examine Address Byte #2 of the LAPD header of frame 100 (another ISDN Setup Unrestricted Digital request) and compare it with that of frame 3, you'll see that the brouter is trying to use the other TEI assigned to it. Examine the Summary window decode for frame 100: is the telephone number called the same or different from that of frame 3?

12. From the Summary window, which B channel is being added in frame 110?

13. Determine in which frames the brouter issues an ISDN Connect and the ISDN network issues the appropriate "ack"?

14. Position your **cursor** on the DLC Header of frame 161. Which B channel is being used to carry the data? Use **F8** continuously until you see the first use of the second B channel, B2. Which frame did you find it in and who was using the channel: the brouter for in-band communication management or the LAN devices to move data?

ISDN Exercise 1

Continued

15. In which frame do we see the second B channel being used by the LAN devices to move data? Continue to use **F8** to move from frame to frame. What do you notice about the "loading" of each B channel? What is the facility called that permits both B channels to be activated to accommodate an increase in network load?

ISDN Exercise 2

Objective: To perform basic troubleshooting of BRI ISDN.

Background: The ISDN configuration is for both voice and data channels.

1. **Load** and **display** the trace file C:\SYCAP\TC107\SPEECH2.SYC. Press **F3** twice to display the data.

2. Press **F5** for Main Menu, **cursor down** to Options, and then **cursor right**. Set the **Frame Type** to Router/Bridge and the **Line Interface** to ISDN BRI. Press **F3** twice to display the data.

3. Change the **Display Options** to display **Summary** and **Detail** windows, set the **Name Width**=9, and enable **DLC Addresses** and **Two-station Format**. Press **F3** to display the data.

4. Use **F6** for Display Options and set a protocol display filter for just ISDN. Press **F3** to display the frames. Your Sniffer Analyzer screen is now "optimized" for viewing ISDN.

ISDN Exercise 2

Continued

5. In the Summary window decode of frame 10, notice the telephone number the router is calling from is 510-919-2234. Is this a data channel call or a speech channel call? Looking at the Detail window at the Call Reference Field of the ISDN Call Control header, what is the reference number for this call?

6. What is unusual about the called telephone number of frame 10?
   Does this justify the ISDN Disconnect message of frame 13?
   What changes would need to be made so that this situation does not repeat itself?

7. In frame 212, we see the router issue a call to the proper called telephone number. Looking at the Detail window at the Call Reference field of the ISDN Call Control header, what is the reference number for this call?
   Why didn't the call go through? (look at frame 214)

In Summary...

- The Sniffer Internetwork Analyzer with ISDN protocol analysis **monitors the D channel of a PRI** in real time.
- The Sniffer Internetwork Analyzer with ISDN protocol analysis **allows simultaneous monitoring of the 2 B channels and 1 D channel monitoring of a BRI** in real time.
- The Sniffer is inserted into a primary or basic rate circuit using pods that allow the traffic to be copied to the Sniffer.
- The Analyzer can be used to troubleshoot:
  - Router disconnection problems.
  - Quality of Service differences.
  - Vendor incompatibilities.

X.25

Objectives

On completion of this section you will:

- Understand how the communications components work together to transmit and receive data using X.25 protocols.
- Know the specifics of the various specifications for tasks in the X.25 suite of protocols.
- Recognize the features of the connection types.
- Be able to analyze the phases within a packet exchange.
- Know how to correlate Logical Channel Numbers (LCNs) with permanent or virtual circuits.
- Be able to identify the fields in the frames that assist you to troubleshoot a connection.

X.25 History

- Conceived of as a protocol to allow a standard interface to a packet switched network not based on any vendor's (HP, DEC, IBM) proprietary data communication protocols.
- Developed primarily from direction received by the European telecommunications organizations.
- Original document based on recommendations from three new packet switching networks: Datapac (Canada), and Tymnet and Telenet (US).
- First published version was in 1974 by CCITT and known as the "Gray Book".
- Numerous revisions since. Current release is the 1988 "Red Book Recommendation".

Historically, X.25 was revised every four years. In 1988, the CCITT announced it would make revisions more frequently if needed.

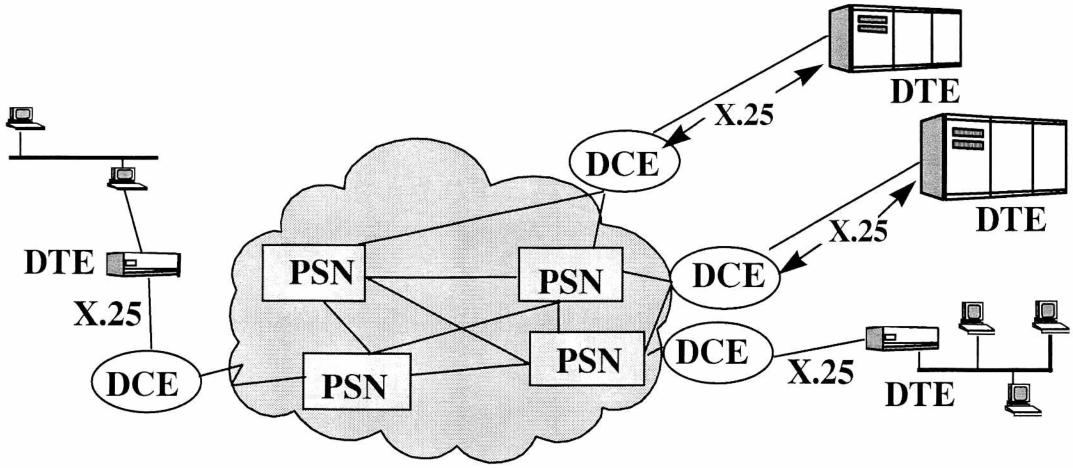
X.25 Overview

- Primary wide area interface standard worldwide providing reliable end-to-end packet transmission.
- Called the *X.25 Recommendation* by CCITT.
- Procedures defined between DTE and DCE are connection establishment, data exchange, and connection close .
- Procedures include such functions as acknowledging packets, requesting retransmissions of error packets, and providing flow control.

CCITT avoids using terms like "**standard**" to avoid giving the impression that its specifications are required.

One of the biggest differences in a Recommendation and a Standard is timeframe to develop it.

DTE and DCE



X.25 only defines procedures for transferring data between the DTE and the DCE. It's up to other protocols to govern communication within the cloud.

A DCE provides the network interface to the DTE. In this context, the DTE is typically a router or PAD (Packet Assembler/Disassembler). The DCE is usually an X.25 network interface switch.

It is important to know that X.25 does not define the details of the network. X.25 defines a packet switched network which is *accessed* by a protocol compliant with the X.25 Recommendation. X.25 only guarantees end-to-end connectivity if both sides are using X.25; it does not guarantee they will exchange meaningful upper layer protocol data.

X.75 governs communication between two X.25 packet switching networks.

The Packet Assembler/Disassembler (PAD)

- Interfaces asynchronous terminals to synchronous network.
- Assembles terminal characters into the information field of the packet for transmission over X.25 network.
- Disassembles the information field back to individual characters at the other end.
- Handles virtual call setup and clearings.
- Automatically detects terminal's data rate, parity setting, and code type.

On most modern networks, virtual call setup, call clearing, and the muxing of multiple LCNs onto the serial link is handled by the routers at either end of the WAN.

PAD Related Recommendations

- **X.3** defines the PAD parameters such as flow control, operating speed, echoing of characters, etc. for communication with an asynchronous terminal.
- **X.28** defines the language by which the terminal communicates with the PAD. Terminals can send **command signals** to the PAD to set up and tear down calls and reconfigure the X.3 table. PADs can also send control messages called **service signals**.
- **X.29** defines the procedures for the PAD and remote DTE or PAD to exchange control information over an X.25 call.

The 1988 version of X.3 defines a set of 22 parameters that the PAD uses to identify and control each terminal communicating with it. When a DTE/DCE connection is to established, the PAD parameters are used to determine how the PAD communicates with the user DTE and vice versa. The user DTE also has the option of altering the parameters after the logon to the PAD device is complete. Each of the 22 parameters consists of a reference number and parameter values.

X.28 - A control-P (Data Latch Enable character) is used to talk to PAD.

X.3 PAD Parameters

X.3 Parameter #	Description
1 Pad recall	Escape from data transfer mode to command mode in order to send PAD.
2 Echo	Controls the echo of characters sent by the terminal.
3 Data forwarding	Defines the characters to be interpreted by the PAD as a signal to forward data.
4 Idle timer	Selects a time interval between successive characters of terminal activity as a signal to forward data.
5 Ancillary device control	Allows the PAD to control the flow of terminal. data using XON/XOFF characters.
6 Control of PAD signals	Allows the terminal to receive PAD service messages.

X.3 PAD Parameters

Continued

X.3 Parameter #		Description
7	**Operation of PAD on receipt of break signal from DTE**	Allows PAD action when a break signal is received from the terminal.
8	**Discard output**	Controls the discarding of data pending output to a terminal.
9	**Padding after carriage return**	Controls PAD insertion of padding characters after a carriage return is sent to a terminal.
10	**Line folding**	Specifies whether the PAD should fold the output line to the terminal.
11	**Binary speed of the DTE**	Indicates the speed of the terminal. Cannot be changed by DTE.
12	**Flow control of the PAD**	Allows the terminal to flow control data being transmitted to the PAD.

X.3 PAD Parameters

Continued

X.3 Parameter #	Description
13 Line feed insertion	Controls PAD insertion of line feed after carriage return is sent to the terminal.
14 Line feed padding	Controls PAD insertion of padding characters after a line feed is sent to the terminal.
15 Editing	Controls whether editing by PAD is available during data transfer mode (parameters 16, 17, and 18).
16 Character delete	Selects character used to signal character delete.
17 Line delete select	Selects character used to signal line delete.
18 Line display	Selects character used to signal line display.
19 Editing PAD service signals	Controls the format of the editing PAD service signals.
20 Echo mask	Selects the characters which are echoed to the terminal when echo (Parameter 2) is enabled.

X.3 PAD Parameters

Continued

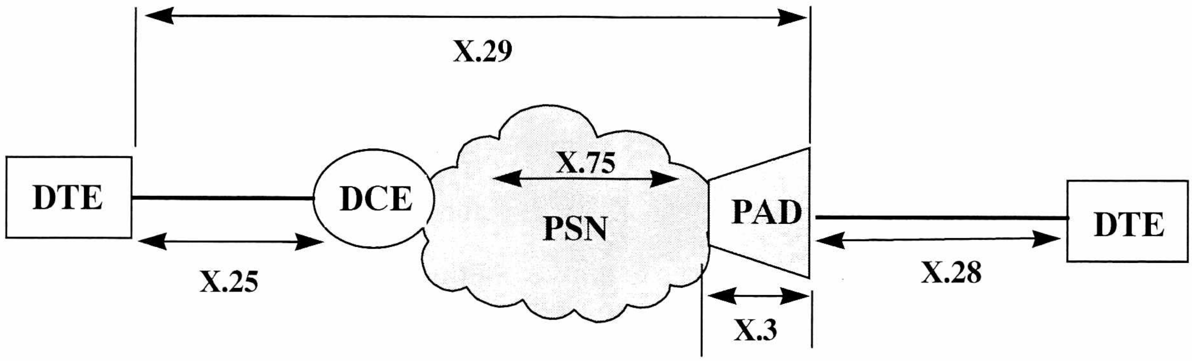
X.3 Parameter #	Description
21 Parity treatment	Controls the checking and generation of parity on characters from/to the terminal.
22 Page wait	Specifies the number of lines to be displayed at one time.

X.3 Parameters

Continued

```
DETAIL
PAD:  ----- X.3/X.29 (PAD) Protocol -----
PAD:
PAD:  Message code = 0 (Parameter indication)
PAD:  Reference = 1 (PAD recall using a character)
PAD:  Value     = 1 (Possible by character DLE)
PAD:  Reference = 2 (Echo)
PAD:  Value     = 1 (Do echo)
PAD:  Reference = 3 (Data forwarding signals)
PAD:  Value     = 7E
PAD:  .1.. .... = All other characters in columns 0 and 1
PAD:  ..1. .... = HT, LF, VT, FF
PAD:  ...1 .... = ETX, EOT
PAD:  .... 1... = DEL, CAN, DC2
PAD:  .... .1.. = ESC, BEL, ENQ, ACK
PAD:  .... ..1. = CR
PAD:  .... ...0 = Not alphanumeric characters
PAD:  Reference = 4 (Idle time delay)
PAD:  Value     = 0 (No data forwarding on time-out)
PAD:  Reference = 5 (Ancillary device control)
PAD:  Value     = 1 (Use of X-ON and X-OFF - data transfer)
                          Frame 2 of 21
                  Use TAB to select windows            File: PAD.SYC
1      2 Set  3Expert 4 Zoom 5      6Disply 7 Prev 8 Next 9Select 10 New
 Help   mark  window   out   Menus  options frame  frame  frame  capture
```

PAD Protocols



(Source: X.25: The PSN Connection, Hewlett Packard)

X.121 describes the 14 digit addressing scheme to allow users on one network to dial users on another network.

X.75 allows any network to talk to any other network within the cloud, for example, Telenet to Tymnet to Datapac.

X.29 Control Messages

Type	Value	Meaning
Set	2	Change an X.3 value.
Read	4	Read an X.3 value.
Set and Read	6	Change an X.3 value and require PAD to confirm change.
Parameter Indication	0	Response to above commands.
Invitation to clear	1	Remote DTE can clear call, PAD clears local terminal.
Indication of break	3	PAD indicates terminal had transmitted break signal.
Error	5	Response to invalid PAD message.

Demonstration file:
C:\SYCAP\TC107\PAD.SYC
Turn off Symptoms. Set Display protocol filter to show only PAD. Notice that X.3/X.29 sits on top of X.25 in the data portion of the frame.

In frame 1, the DTE issues a command to read the X.3 table. In frame 3, the DTE issues a Set and read to change an X.3 value and require the PAD to confirm. The Parameter indication is the response to both these commands. If you turn on Two viewports and compare the Detail windows of frames 2 and 6, you will notice that the Operation of PAD on receipt of break signal was changed to a Value=0 meaning the PAD should do nothing. Frame 7 is a Set only, which does not require the PAD to confirm the change. The rest of the frames are data.

Packet Switched Networks

- **PSN - Packet Switched Network:** Provides a service to users of data networks who in turn pay the PDN administration for its use.
  - Aliases include:
    - PPN Public Packet Network
    - PPSN Public Packet Switched Network
    - PDN Public Data Network
- **Packet switching** is a transmission method used by PSNs whereby each packet can be switched over a different route through the network, to compensate for link or switch congestion and outages. This is in contrast to *circuit* switching, in which one call uses the same path for the duration of the call.

Types of Connections

- **Virtual circuits:** X.25 uses statistical time-division multiplexing to packet interleave multiple users' data onto a single communications link. The user perceives an end-to-end dedicated line.
- **Physical circuits:** The communications line between devices.
- **Logical channel:** The local connection between the user DTE and the network DCE. Each side of the network has a logical channel and the network maps the logical channels to a virtual circuit.

Upon establishing a connection to or from the network, the DTE or the DCE assigns a logical channel number (LCN) to identify the connection.

X.25 Layers

X.25 Protocol Stack		OSI Model Lower Three Layers
X.25	**Packet Level**	Network
LAPB OR LAPD	**Frame Level**	Data link
X.21, X.21 *bis*, or V-Series Recommendations	**X.25 Level 1**	Physical

SNIFFER® UNIVERSITY

X.25 11 - 17

Internetwork Analysis and Troubleshooting, 10/96, Rev. 5.0

X.25 at Level 1

- CCITT defines X.21 *bis* as a point-to-point, synchronous, full-duplex communications link functionally equivalent to EIA RS-232C (US.) and CCITT V.24/V.28 in Europe.
- X.21 *bis* and X.21 are defined between the DTE and DCE.
- X.21 *bis* allows connecting a DTE to the network via an analog modem.
- X.21 *bis* currently more widely implemented than X.21 which only runs over a digital link.
- CCITT Recommendation V.35 forms the basis for X.21 *bis* for transmission speeds greater than 48000 bps.

X.25 at the Frame Level

- Also called the Link Level, ensures error-free frame delivery between the user DTE and the network.
- Several varieties exist:
  - Earlier X.25 versions use Link Access Procedure (LAP) or binary synchronous (bisync).
  - Today most use Link Access Procedure Balanced (LAPB).
  - Link Access Procedure for the ISDN D-channel (LAP-D) use is increasing.
  - For LANs carrying X.25 traffic, the Logical Link Control (LLC) layer is used.
- X.25 at the link level is a combination of hardware and software and some implementations are available on a chip set.

Fortunately, these data link layer protocols all are derived from ISO's High-Level Data-link Control (HDLC) so knowing one makes you an instant expert on all of them. Well, maybe it's not quite that simple but...

X.25 at the Frame Level

Continued

```
SUMMARY—Delta T—DST—————————————SRC——————————————————————————————————————————————
M    1               DCE.LCN.008      «DTE.LCN.008       DLC DTE->DCE Length=6
                                                          HDLC R I    NR=2 NS=2 P/F=
                                                          X.25 008 Data PR=0 PS=0 Q
                                                          PAD C Read
     2    0.0317     DTE.LCN.008      «DCE.LCN.008       DLC DCE->DTE Length=50
                                                          HDLC R I    NR=3 NS=3 P/F=
                                                          X.25 008 Data PR=1 PS=0 Q
                                                          PAD R Parameter 1=01 2=01
     3    0.0220     DCE.LCN.008      «DTE.LCN.008       HDLC retransmission
———————————————————————————————Frame 1 of 21—————————————————————————————————————
DETAIL
 HDLC: ----- High Level Data Link Control (HDLC) -----
 HDLC:
 HDLC: Address = 03 (Response)
 HDLC: Control field = 44
 HDLC:     010. .... = N(R) = 2
 HDLC:     ...0 .... = Poll/Final bit
 HDLC:     .... 010. = N(S) = 2
 HDLC:     .... ...0 = I (Information transfer)
 HDLC:
———————————————————————————————Frame 1 of 21—————————————————————————————————————
                          Use TAB to select windows                File: PAD.SYC
1        2 Set   3Expert  4 Zoom   5        6Disply  7 Prev   8 Next   9Select  10 New
  Help     mark   window    in       Menus   options   frame    frame    frame   capture
```

X.25 at the Packet Level

```
DETAIL
 HDLC:      .... ...0 = I (Information transfer)
 HDLC:
 X.25: ----- X.25 Packet Level -----
 X.25:
 X.25: General format id = 90
 X.25:          1... .... = Qualifier bit
 X.25:          .0.. .... = Delivery confirmation bit
 X.25:          ..01 .... = Sequence numbering modulo 8
 X.25:          .... 0000 = Logical channel group number = 0
 X.25: Logical channel number = 08
 X.25: Data packet info = 00
 X.25:         000. .... = P(R) = 0
 X.25:         ...0 .... = More bit
 X.25:         .... 000. = P(S) = 0
 X.25:         .... ...0 = Packet type identifier (Data)
 X.25:
 PAD:  ----- X.3/X.29 (PAD) Protocol -----
 PAD:
 PAD:  Message code = 4 (Read)
 PAD:
                              Frame 1 of 21
                         Use TAB to select windows                File: PAD.SYC
1      2 Set  3Expert 4 Zoom 5       6Disply 7 Prev  8 Next  9Select 10 New
 Help   mark  window   out    Menus  options  frame   frame   frame  capture
```

LAPB

- Supports only full-duplex, point-to-point, non-switched channels because an X.25 link is only between the user DTE and the attached packet switched DCE.
- Supports combined-station approach, balanced configuration, and the asynchronous balanced communication mode.
- Frame format identical to HDLC with one exception: control field can be 2 bytes long, allowing for extended sequencing.
- X.25 specifies LAPB address fields designate the DTE as A and DCE as B (A=03, B=01).

Demonstration file:
C:\SYCAP\TC107\DEMO_X25.SYC
Most implementations do not use the two byte control field for extended sequencing. They use "standard" HDLC with a one byte control field.

Combined station	Peer-peer approach.
Balanced configuration	Both stations responsible for link maintenance.
Asynchronous balanced mode	Combined station may initiate transmissions without receiving permission.

LAPB (HDLC)

```
DETAIL
HDLC: ----- High Level Data Link Control (HDLC) -----
HDLC:
HDLC: Address = 03 (Response)
HDLC: Control field = 44
HDLC:      010. .... = N(R) = 2
HDLC:      ...0 .... = Poll/Final bit
HDLC:      .... 010. = N(S) = 2
HDLC:      .... ...0 = I (Information transfer)
HDLC:
X.25: ----- X.25 Packet Level -----
X.25:
X.25: General format id = 90
X.25:          1... .... = Qualifier bit
X.25:          .0.. .... = Delivery confirmation bit
X.25:          ..01 .... = Sequence numbering modulo 8
X.25:          .... 0000 = Logical channel group number = 0
X.25: Logical channel number = 08
X.25: Data packet info = 00
X.25:         000. .... = P(R) = 0
X.25:         ...0 .... = More bit
                              Frame 1 of 21
                         Use TAB to select windows                File: PAD.SYC
1      2 Set  3Expert 4 Zoom  5      6Disply 7 Prev  8 Next  9Select 10 New
 Help   mark  window   out   Menus  options  frame   frame   frame  capture
```

Three Phases of Frame Exchange

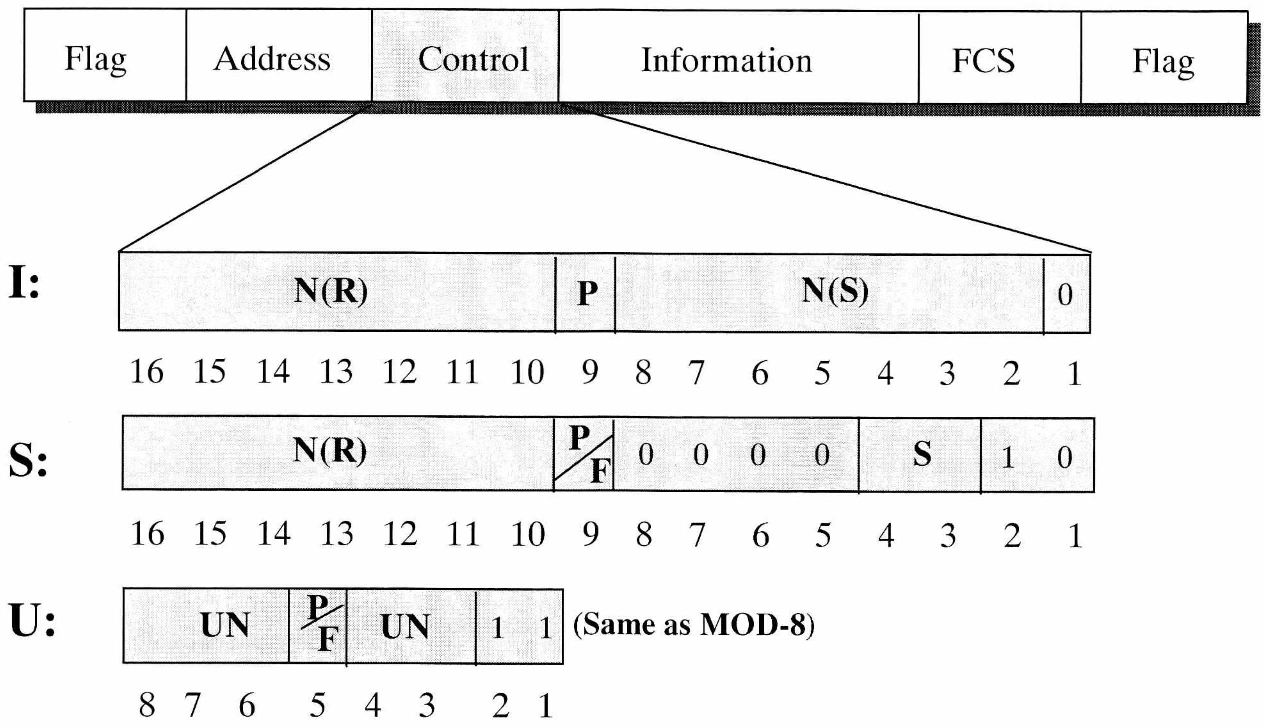
- **Link Setup Phase**
  - DTE/DCE wishing to communicate issues an Unnumbered command frame (SABM) and waits for an Unnumbered response frame (UA).
- **Information Transfer Phase**
  - Information frames (packets) are checked for errors and proper sequencing which is accomplished at frame level, typically using Modulo-8.
  - Supervisory frames are used to acknowledge received frames, control data flow and frame retransmission of erred or lost frames.
- **Link Disconnect Phase**
  - Ensures information transfer is complete and then logically disconnects the link.
  - DTE/DCE wishing to discontinue communication issues an Unnumbered command frame (DISC) and awaits an Unnumbered response frame (UA).

Demonstration file:

C:\SYCAP\TC107\DEMO_X25.SYC.

If you set a display protocol filter for HDLC, you can see the Link Setup and Information Transfer Phases starting at frame 1. This trace does not show the Link Disconnect Phase.

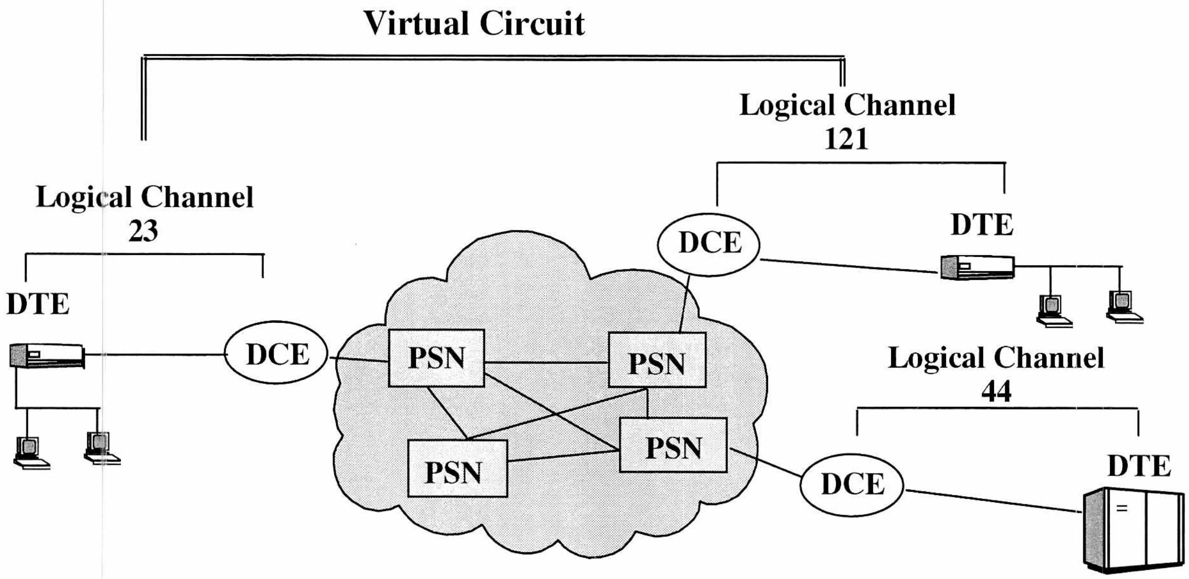
LAPB Frame with Extended Sequencing



This slide is included for reference. As mentioned, most WAN implementations do not use extended sequencing.

Note: LLC Type 2 does use extended sequencing.

Logical Channel Numbers (LCNs)



X.25 uses logical channel numbers to identify each active PVC or SVC on a DTE/DCE interface, thereby allowing many virtual circuits to exist over the same physical link. LCNs have local significance only. Since the length of the LCN field is 12 bits long, as many as 4095 LCNs per DTE/DCE interface are possible (0 is reserved for DCE use). However, in practice the number is far lower.

It is the network administrator's responsibility to determine how these LCNs get mapped to a local interface. X.25 does not define how this should take place.

In addition, the switching of packets from one LCN to another is not defined by X.25, and is handled by the switching tables within each PSN node.

LCNs
Continued

- For PVCs, the LCN is assigned at the time of subscription.
- For SVCs, the LCN is assigned when the call is initiated.
- To avoid packet collisions, the DTE assigns LCNs from the top down, while the DCE assigns LCNs from the bottom up.
- In the case of a collision (the same LCN assigned by the DTE and DCE simultaneously), the incoming call packet from the remote DTE is cleared, while the outgoing call request from the local DTE is processed normally.

X.25 Packet Structure

	Byte	Bits 8 7 6 5	Bits 4 3 2 1
Basic X.25 Header	1	General Format Identifier	Logical Channel Group Number
	2	Logical Channel Number	
	3	Packet Type Identifier	
Packet type dependent		Calling DTE Address Length	Called DTE Address Length
		DTE Address Field	
		Facility Field	
		User Data	

We will look at these frames in more detail in the next few pages.

General Format Identifier (GFI)

Bits	8	7	6	5	4	3	2	1
Byte 1	Q	D	Sequence Number		LCGN			

Sequence Number	
01	Modulo 8
10	Modulo 128
11	Extensions
00	Reserved

Q bit (Qualifier bit) Used by X.25 to qualify the data in the information field.
Q=1 indicates the data being sent is significant to the remote DTE. Useful when the remote DTE is connected to the network via a PAD and data packets to the remote DTE need to be distinguished from control packets to the PAD.

D bit (Delivery confirmation bit) Used in call setup and data packets.
D=1 allows a DTE to request an acknowledgment from the remote DTE. Called end-end acknowledgment.
D=0 is for normal operation. Local acknowledgment is from the DCE.

Demonstration file:
C:\SYCAP\TC107\DEMO_X25.SYC
Set a display filter to show X.25 as the highest layer protocol. Look at the frames with the Q bit set and compare them to frames in which this bit is not set. Is this implementation of X.25 setting the Q bit for data or control packets? and is it being set consistently?
The D bit is not widely implemented.

Look at the frames with the Q bit set. The local DTE sets the Q bit, if it is to be used, to the same value (either 0 or 1) for all DATA packets of the corresponding sequence.
Recommendation X.25 does not specify the Q bit be set to a 1 or a 0, only that they be set the same for all data packets. Otherwise, the value set is not guaranteed preservation and some networks may even reset the virtual circuit call or permanent virtual circuit if these bits are not implemented consistently.

Logical Channel Identifier

Bits	8	7	6	5	4	3	2	1
Byte 1	GFI				**Logical Channel Group Number**			
2	**Logical Channel Number**							
3	Packet Type Identifier							

- 4095 LCNs are possible. 0 is reserved for DCE control use.
- LCNs are split into four groups: three for SVCs and one for PVCs.
  - **Permanent virtual circuits:** (LCN assignments begin here.)
  - **One-way incoming:** DTEs can receive but not initiate calls.
  - **Two-way:** DTEs can receive and send calls.
  - **One-way outgoing:** DTEs can initiate calls but not receive them.
- X.25 does not specify the size of the groups, only that LCNs within a group be contiguous. X.25 also recommends a range of LCNs be left unassigned between groups.

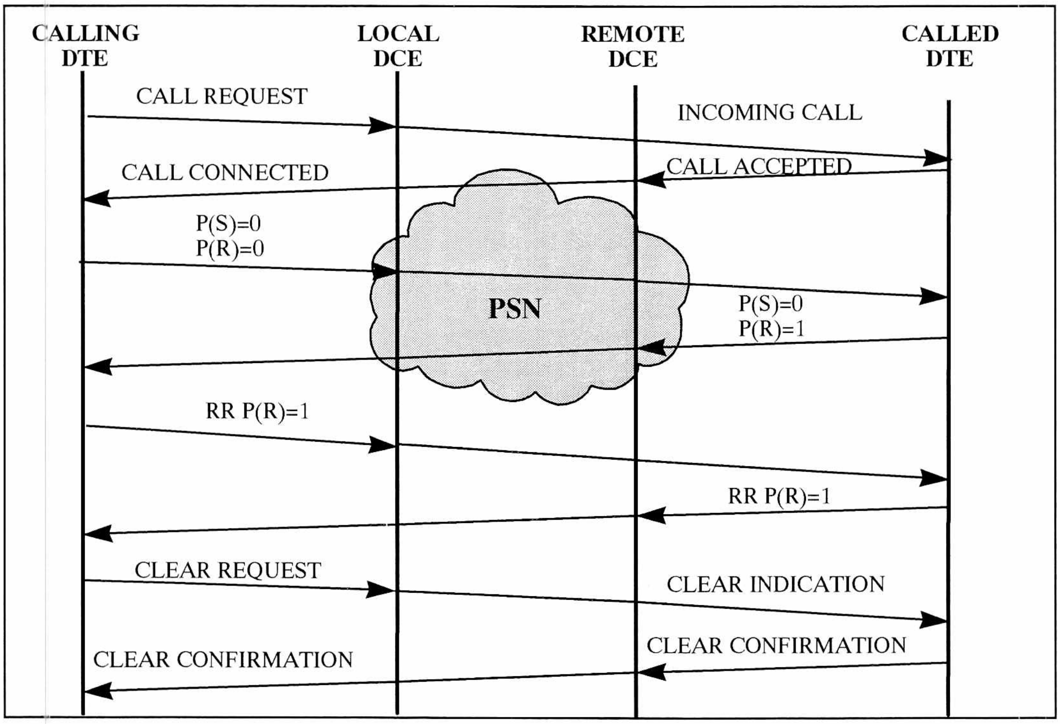
Demonstration file:
C:\SYCAP\TC107\X25CALL.SYC
In frame 3, the DTE places a call on logical channel number (LCN) 032.

LCN

Continued

```
DETAIL
X.25: ----- X.25 Packet Level -----
X.25:
X.25: General format id = 10
X.25:         0... .... = Address bit (non-TOA/NPI address)
X.25:         .0.. .... = Delivery confirmation bit
X.25:         ..01 .... = Sequence numbering modulo 8
X.25:         .... 0000 = Logical channel group number = 0
X.25: Logical channel number = 32
X.25: Packet type identifier = 0B (Call request)
X.25: Address length field = AA
X.25:            1010 .... = Calling DTE address length = 10 digits
X.25:            .... 1010 = Called  DTE address length = 10 digits
X.25: Called  DTE address = 4152574300
X.25: Calling DTE address = 4152574300
X.25: Facility length = 0
X.25: Protocol identification = 01000000 (PAD)
X.25:
X.25: [4 bytes of user data = 01000000]
X.25:

                          Frame 85 of 4059
                      Use TAB to select windows              File: SUNX253.SYC
1      2 Set  3Expert 4 Zoom  5       6Disply 7 Prev  8 Next  9Select 10 New
 Help   mark  window   out     Menus  options  frame   frame   frame  capture
```

Basic Packet Exchange



Three Phases of Packet Exchange

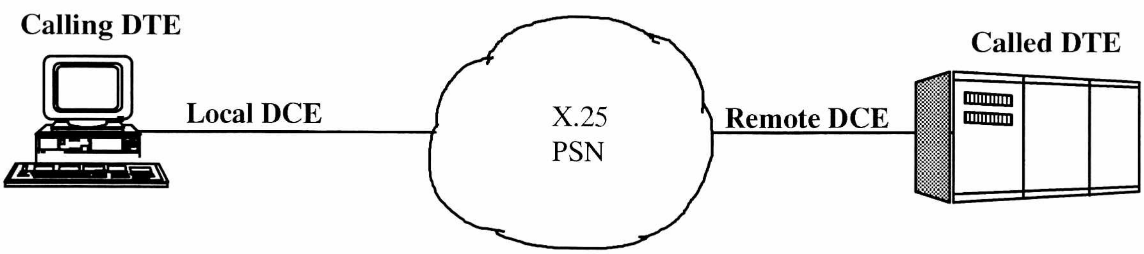
- **Call Setup**
  - **calling DTE** CALL REQUEST packet becomes INCOMING CALL packet to **called DTE.**
  - **called DTE** CALL ACCEPTED packet becomes CALL CONNECTED packet to **calling DTE.**
- **Data Transfer**
  - information spanning more that one packet is split between subsequent packets with the M- or More-bit set.
  - local (local DTE to local DCE, remote DCE to remote DTE) and/or end-to-end (local DTE to remote DTE) acknowledgments use the D-bit reset (0) or set (1), respectively.
  - network layer packet sequencing - P(S), P(R) - is used independently of data link layer frame sequencing.
- **Call Clearing**
  - **calling DTE** CLEAR REQUEST packet becomes CLEAR INDICATION packet to the **called DTE.**
  - **called DTE** CLEAR CONFIRMATION packet is returned to the **calling DTE.**

Demonstration file:

C:\SYCAP\TC107\X25CALL.SYC

Turn off Symptoms; set display filter for X.25. Frames 3 and 4 show the Call Setup packets. Frames 5-36 show Data Transfer; frames 37 and 38 show the Call Clearing**.**

Either the DTE or DCE can initiate any of the three phases of packet exchange at the network layer.



Three Phases of Packet Exchange

Continued

```
SUMMARY—From DTE————From DCE——————————————————————————————————
 4027  X.25 032 Call Req Called:031344152574301 Calling:4152574300 PAD
 4029                X.25 001 Inc Call Called:031344152574301 Calling:03134
 4030  X.25 001 Call Acc
 4032                X.25 032 Call Cnct Facils=2
 4034  X.25 032 Data PR=0 PS=0
 4036                X.25 001 Data PR=0 PS=0
 4037                X.25 032 RR   PR=1
 4038  X.25 001 RR   PR=1
 4040  X.25 032 Data PR=0 PS=1
 4042                X.25 001 Data PR=0 PS=1
 4043                X.25 032 RR   PR=2
 4044  X.25 001 RR   PR=2
 4046  X.25 032 Data PR=0 PS=2
 4048                X.25 001 Data PR=0 PS=2
 4049                X.25 032 RR   PR=3
 4050  X.25 001 RR   PR=3
 4053  X.25 032 Clr Req DTE originated
 4055                X.25 001 Clr Ind DTE originated
 4056                X.25 032 Clr Conf
 4057  X.25 001 Clr Conf
——————————————————————Frame 4027 of 4059——————————————————————
                    Use TAB to select windows            File: SUNX253.SYC
1       2 Set   3Expert  4 Zoom  5         6Disply 7 Prev  8 Next  9Select 10 New
  Help    mark  window    out     Menus    options   frame   frame  frame  capture
```

Packet Type Identifier

Function	Packet Type (Byte 3) From DTE to DCE	From DCE to DTE	Bit Values 8 7 6 5 4 3 2 1
Call Setup and Clearing	Call request	Incoming call	0 0 0 0 1 0 1 1
	Call accepted	Call connected	0 0 0 0 1 1 1 1
	Clear request	Clear indication	0 0 0 1 0 0 1 1
	Clear confirmation	Clear confirmation	0 0 0 1 0 1 1 1
Data Transfer and Interrupt	Data	Data	x x x x x x x 0
	Data interrupt	Data interrupt	0 0 1 0 0 0 1 1
	Intrpt confirmation	Intrpt confirmation	0 0 1 0 0 1 1 1
Flow Control	Receive ready	Receive ready	x x x 0 0 0 0 1
	Receive not ready	Receive not ready	x x x 0 0 1 0 1
	Reject	does not exist	x x x 0 1 0 0 1
Reset a Virtual Circuit	Reset request	Reset indication	0 0 0 1 1 0 0 1
	Reset confirmation	Reset confirmation	0 0 0 1 1 1 1 1
Restart all Virtual Circuits	Restart request	Restart indication	1 1 1 1 1 0 1 1
	Restart confirmation	Restart confirmation	1 1 1 1 1 1 1 1
	Diagnostic		1 1 1 1 0 0 0 1

By convention, the name of the packet changes depending on whether it is sent from DTE or from DCE. For example, when the *calling* DTE sends a **CALL REQUEST** the *called* DTE receives an **INCOMING CALL** packet.

Demo file:
C:\SYCAP\TC107\SISUNX25.SYC.
Set display filter for X.25.
Frame 85 [CALL REQUEST from the DTE]
Frame 87 [INCOMING CALL from the DCE]

Data Packet Control Field

Bits 8	7	6	5	4	3	2	1
Packet receive sequence P(R)			**M bit**	**Packet send sequence P(S)**			0

Always 0 for data packet

P(S) and P(R): similar to N(S) and N(R) at layer 2 but work **independently** of layer 2. Can be Mod-8 or Mod-128.

M or More bit allows fragmentation when packets are larger than the X.25 MTU (maximum transmission unit).

Demonstration file:

C:\SYCAP\TC107\X25CALL.SYC.

Turn off Symptoms.

Set a display protocol filter for X.25 and HDLC and turn on All layers.

Follow the sequenced packet exchange at both layers 2 and 3.

Packet Summary

- The 15 Packets Types can be categorized into 4 groups according to function:
  - **Call Setup and Clearing** packets -
    - These provide session establishment and clearing. They are only used on SVCs.

- CALL REQUEST	- INCOMING CALL
- CALL CONNECTED	- CALL ACCEPTED
- CLEAR REQUEST	- CLEAR INDICATION
- CLEAR CONFIRMATION	

  - **Data Transfer and Maintenance** packets -
    - These packets are used to carry data, provide flow control, and to provide an interrupt capability during data transfer.

- DATA	- P(REJ)
- P(RR)	- P(RNR)
- DATA INTERRUPT	- INTERRUPT CONFIRMATION

Demo File:

C:\SYCAP\TC107\X25CALL.

SYC Frame 37 shows a CLEAR REQUEST packet and frame 38 shows a CLEAR CONFIRMATION.
Frame 6 shows the first RR. This trace doesn't have any other Flow Control, Diagnostic, or Interrupt packets.

The RR and RNR perform the same function as in HDLC and can be transmitted by either the DTE or the DCE. The REJ, transmitted only by the DTE, indicates receipt of an out of sequence packet (just like HDLC), however, the REJ packet may or may not be supported by the PSN.

Packet Summary

Continued

- **Virtual Call Maintenance** packets -

  Used for clearing and resetting SVCs and/or PVCs. A RESTART clears all SVCs and PVCs in use. A RESET sets the P(S) and P(R) counters of one virtual call to zero.

  - RESET REQUEST
  - RESET CONFIRMATION
  - RESET INDICATION
  - RESTART REQUEST
  - RESTART CONFIRMATION
  - RESTART INDICATION

- **Diagnostic** packets -

  Issued by the DCE for fault detection.

Demonstration file:

C:\SYCAP\TC107\X25CALL.SYC

Frames 1 and 2 show Restart packets.

X.25 Exercise

Objective: Analyze the cause of data link and network layer inefficiencies.

Background: A DTE can issue a RESTART REQUEST command at any time to initialize or reinitialize the DTE/DCE interface. Once initialized, the RESTART REQUEST command should only be used for disaster recovery.

1. **Load** the file C:\SYCAP\TC107\SUNX253.SYC

2. Set the **Options, Frame type** to **HDLC then X.25.**

3. Display the data. As we saw earlier, the DCE tries unsuccessfully to establish a session in frames 2-9. What is the normal response to a SABM or SABME?

X.25 Exercise

Continued

4. In this case, what is the DTE's reaction to the SABM?

5. The DTE sets the Poll bit in frames 10 and 11; does the DCE respond with the Final bit set as you would expect?

6. In frames 12-17, the DTE tries to establish a session and the DCE responds with the appropriate UA acknowledgment. Besides the fact that the first attempt was unsuccessful, what else is different between these two attempts at session initialization?

7. What frames show the session establishment is complete at the data link layer?

X.25 Exercise

Continued

8. In frame 61, the DTE attempts to initialize the DTE/DCE X.25 interface by sending a "Restart Normal" (RESTART REQUEST) packet. In frame 63, the DCE forwards a packet - "Restart Network Operational" (RESTART INDICATION) to the Called DTE. What is happening here is that both the end user DTEs are attempting to establish a call. What would be the normal response from either the DTE-DCE or the DCE-DTE interface?

9. What happens instead?

10. What happens in frame 77?

11. Why do you suppose the DCE sends a RNR in frame 79?

X.25 Exercise

Continued

12. What frames show the X.25 DTE/DCE interface successfully initialize?

13. In frames 85 and 87, the DTE places a call to what destination address?

    On what logical channels?

    Is the call accepted?

    What is your hypothesis about the cause?

X.25 Exercise

Continued

14. In frames 88 and 90, the DTE sends CLEAR REQUEST packets to clear the calls. Look in the Detail window of each packet to determine the cause for clearing. What is it?

15. Does this confirm or deny the hypothesis you formulated in question 12?

16. Frames 99 and 101 show a call being placed to 2156901044. Is this call successful?

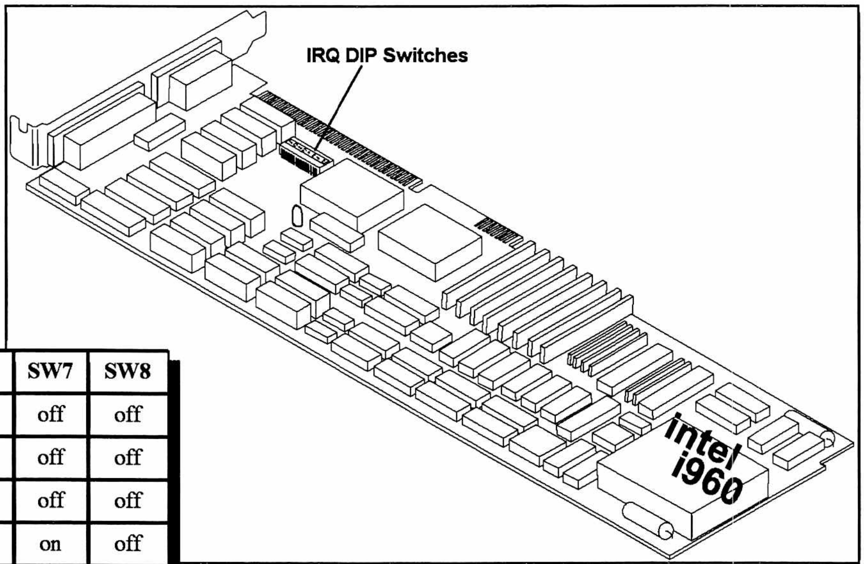
17. Look in the Detail window of frame 99 and note the Protocol identification filed. What upper layer data is this X.25 call going to carry?

Summary

- DTEs, DCEs, PADs work together to transmit and receive data through the PSN using X.25 protocols.
- X.3, X.28 and X.29 define the tasks in X.25.
- Virtual and physical circuits and logical channels comprise the path between devices.
- Packets are exchanged after the link has been set up, then the link is disconnected when the transfer is complete.
- Many virtual circuits can exist on the same physical link by assigning LCNs.

Appendix

Installing the High Speed WAN Card Lab



Line Interface Card Switch Settings:

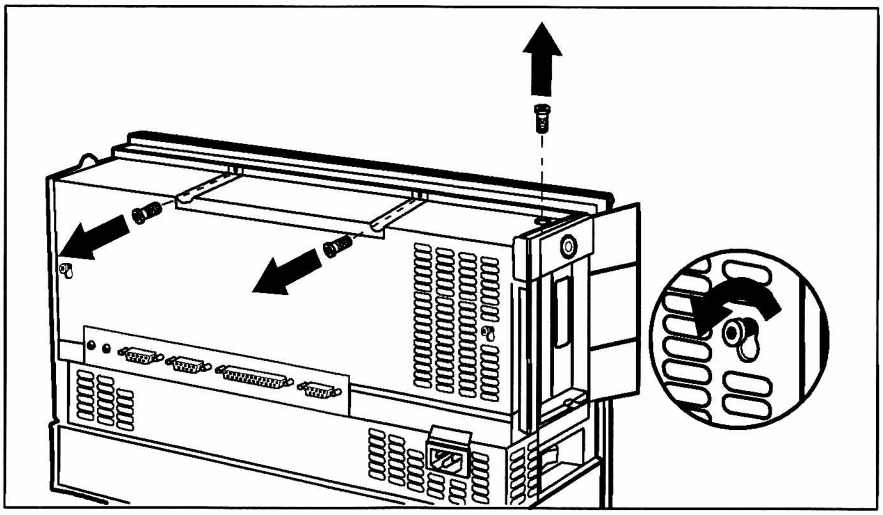
Interrupt #	SW4	SW5	SW6	SW7	SW8
IRQ3	on	off	off	off	off
IRQ4	off	on	off	off	off
IRQ5	off	off	on	off	off
IRQ6	off	off	off	on	off
IRQ7	off	off	off	off	on

Note: IRQ5 is the default for the Sniffer Internetwork Analyzer

Verify that the dip switch settings are set to: Switches **1**, **2**, **3**, and **6** **up** and all the rest **down**.

Installing the High Speed WAN Card Lab

Continued

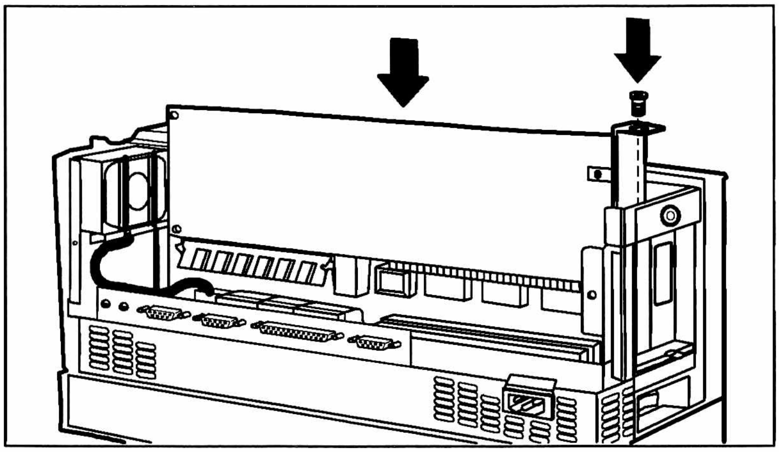


To remove the rear panel and options cover of the Model 54/55 (Compaq 486)...

1. Turn off the computer and disconnect the AC power cord.
2. Rotate the computer so that the rear is facing you and lift the handle on top of the computer. Result: Lifting the handle reveals two Torx T-15 screws on top of the panel.
3. Remove the two Torx T-15 screws on the top of the rear panel.
4. Open the options door on the right side of the computer (if it hasn't already been removed). With the door open, pull on the handle to tilt the rear cover toward you. Lift the cover and lay it down. Result: Removing the plastic rear panel reveals the metal options cover.
5. Remove the three Torx-15 screws securing the top of the options cover to the unit. See the arrows in the above picture.
6. Loosen the two Torx T-15 screws securing the back of the options cover to the unit.
7. With the top screws removed, and the rear screws loosened slide the options cover up and off. Result: Removing the options cover reveals the NIC compartment.

Installing the High Speed WAN Card Lab

Continued



To install a network adapter on the Model 54/55...
Step by step instructions follow. For those familiar with installing adapters on the Compaq 486, you may skip these instructions but **please be careful not to overtighten the retaining screw** when securing the adapter in place.

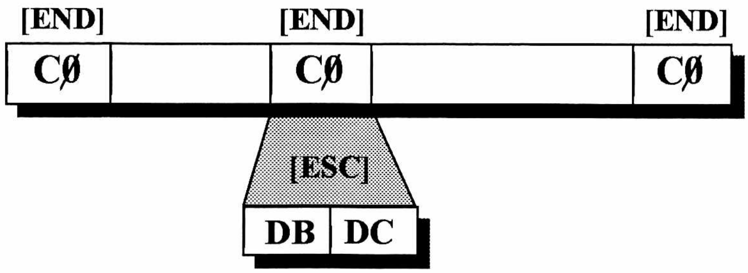
1. Remove the rear panel and options cover (see previous page).
2. There are two adapter cards installed. Please remove the outer one.
3. Remove the Torx T-15 retaining screw at the top of the expansion slot. Lift the expansion slot cover up and out of the computer.
4. Carefully lower the WAN card into the expansion slot and press it firmly until the connectors seat.
5. Reinstall the Torx T-15 retaining screw. **Be very careful not to overtighten the retaining screw: it is possible to strip the threads.**
6. Replace the options cover and rear panel.
7. Power on the computer.

Recommended Reading Materials

1. Black, Uyless, X.25 and Related Protocols, IEEE Computer Society Press, 1991.
2. Flanagan, William A., The Guide to T-1 Networking, 4th edition, Telecom Library Inc., 1990.
3. Hewlett Packard, X.25: The PSN Connection, 1985.
4. Muller, Nathan J. and Davidson, Robert P., The Guide to Frame Relay & Fast Packet Networking, Telecom Library, Inc., 1991.
5. Stalling, William, Networking Standards, A Guide to OSI, ISDN, LAN and MAN Standards, Addison-Wesley Publishing Company, Inc. 1993.
6. Stamper, David A., Business Data Communications, 2nd edition, The Benjamin/Cummins Publishing Company, Inc. 1989.
7. Thorpe, Nicolas M. and Ross, Derek, X.25 MADE EASY, Prentice Hall International (UK) Ltd., 1992.
8. Schlar, Sherman K., Inside X.25: A Manager's Guide, McGraw-Hill, Inc. 1990.

Serial Line Internet Protocol (SLIP)

Serial Line Internet Protocol (SLIP)



- SLIP is a popular method of encapsulating IP traffic over dial-up circuits.
- SLIP contains no addressing, error checking, or control functions. If errors occur on the line, or multiple protocols are to be transmitted, it is up to the higher layer protocols to manage these conditions.
- The IP datagram is terminated with a special character END (C0). Many implementations also place this character at the beginning of the datagram. If the END character appears in the IP text, it is replaced with the ESC sequence; DB and DC.

SLIP has its origins in the 3COM UNET TCP/IP implementation from the early 1980's. It is merely a packet framing protocol; SLIP defines a sequence of characters that frame IP packets on a serial line, and nothing more. It provides no addressing, packet type identification, error detection/correction or compression mechanisms.

The SLIP protocol defines two special characters: END and ESC. END is octal 300 (decimal 192) and ESC is octal 333 (decimal 219) not to be confused with the ASCII ESCape character. For the purposes of this discussion ESC will indicate the SLIP ESC character. To send a packet, a SLIP host simply starts sending data in the packet. If a data byte is the same code as the END character, a two byte sequence of ESC and octal 334 (decimal 220) is sent instead. If it is the same as an ESC character, a two byte sequence of ESC and octal 335 (decimal 221) is sent instead. When the last byte in the packet has been sent, an END character is then transmitted. SLIP is a de facto standard, commonly used for point-to-point serial connections running TCP/IP. It is not an Internet standard.

Maximum Packets on SLIP

Because there is no "standard" SLIP specification, there is no real defined maximum packet size for SLIP. It is probably best to accept the maximum packet size used by the Berkeley UNIX SLIP drivers: 1006 bytes including the IP and transport protocol headers (not including the framing characters). Therefore any new SLIP implementations should be prepared to accept 1006 byte datagrams and should not send more than 1006 bytes in a datagram.

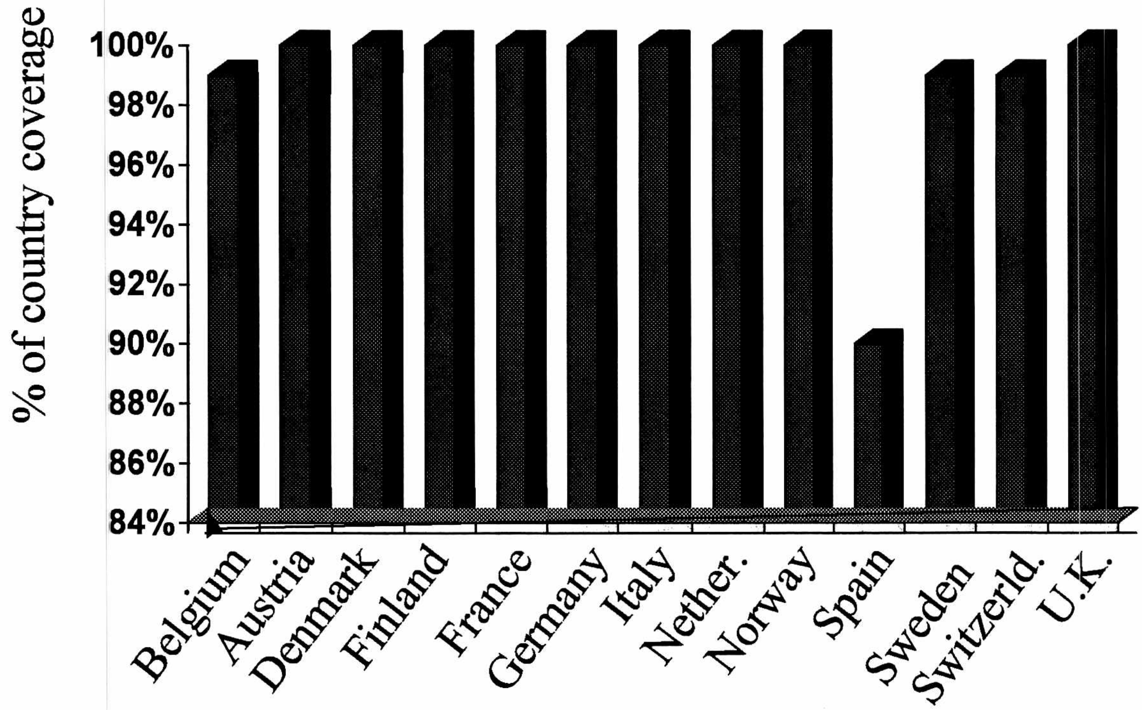
From RFC 1055

Around 1984, Rick Adams implemented SLIP for Berkeley UNIX 4.2 and Sun Microsystems workstations and released it to the world. It quickly caught on as an easy way to connect TCP/IP hosts and routers with serial lines. It is useful today for allowing mixes of hosts and routers to communicate with one another (host-host, host-router, and router-router are all common SLIP configurations).

SLIP for Berkeley UNIX is available via anonymous FTP from the following address **uunet.uu.net in pub/sl.shar.Z**. Be sure to transfer the file in binary mode and then run it through the UNIX uncompress program. Take the resulting file and use it as a shell script for the UNIX /bin/sh (for instance, /bin/sh sl.shar).

EuroISDN

European ISDN Availability



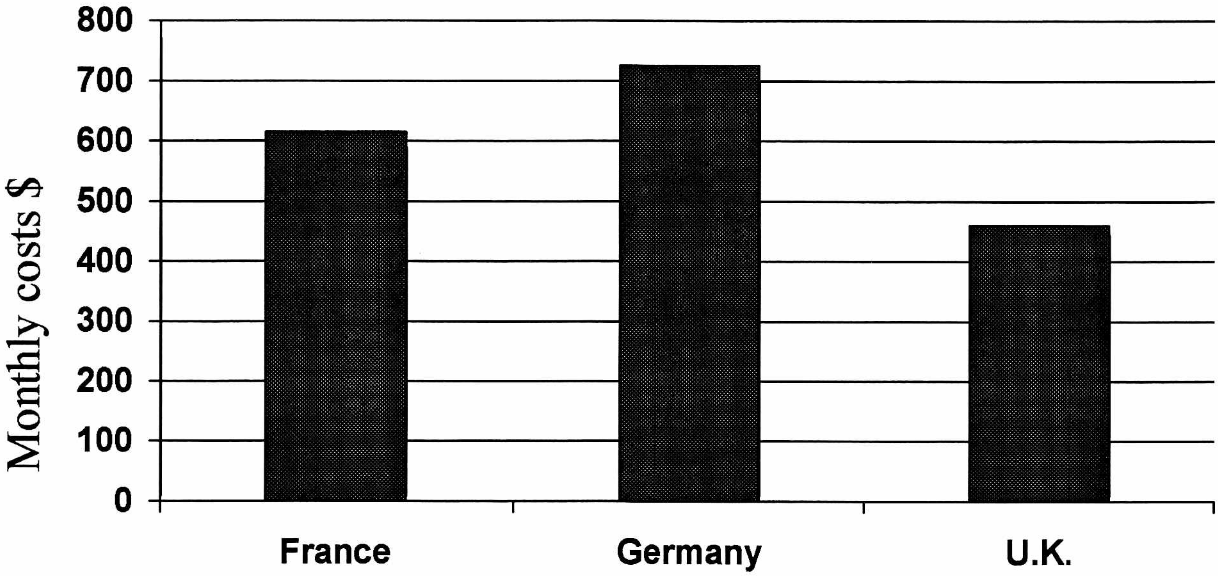
Source: EuroLAN Research '94

ISDN in the European market began in earnest in 1989 with the signing of the Memorandum of Understating (MoU) concerning the deployment of EuroISDN by European PTTs.

ISDN standards were agreed upon demonstrating a real commitment on behalf of the European PTTs to supply an ISDN service and create one standard for Europe.

By mid-1994, nearly all PTTs had ISDN service coverage for the main cities and industrial centers. It is expected that 90% to 100% country coverage will be available before 1998.

Leased Line Monthly Costs
10Km 64Kbps



Source: EuroLAN Research '94

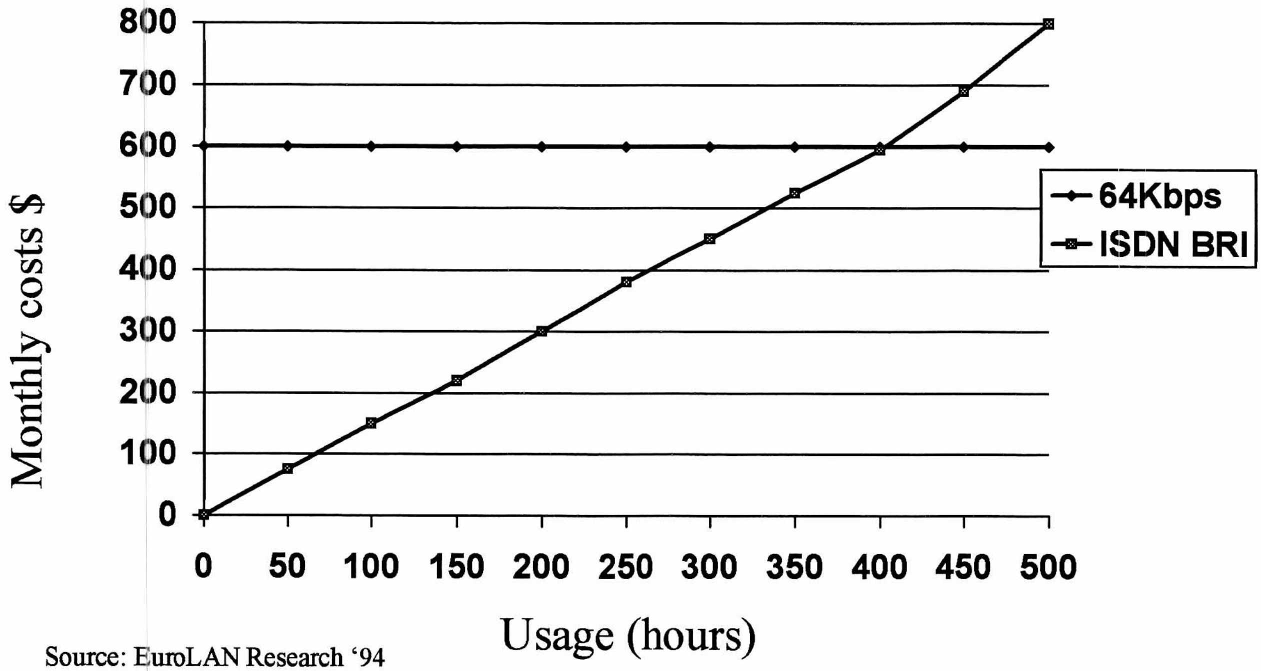
Leased lines are suited to applications where there is a steady stream of data during most of the day. Some applications need instant bandwidth availability that can be provided by the leased line. This same functionality can also be provided by ISDN, with it's short setup time and bit rate increments of 64Kbps.

The general rule is that ISDN becomes viable only when less than 40 hours of usage time per month are used. Depending on the different tariff structures in the different countries, the cost analysis will vary.

Because of the more expensive leased line costs in Germany and France when compared to the U.K., ISDN connections will be more cost effective for a longer period in France and Germany than in the U.K.

If a company is transmitting a large amount of data, then it may be necessary to have two leased lines, even though only one is being used for most of the day. Using ISDN as an alternative to the second leased line is a cheaper solution.

Leased Lines vs. ISDN BRI *Monthly Costs in France*



Source: EuroLAN Research '94

SNIFFER® UNIVERSITY

Appendix 12 - 12

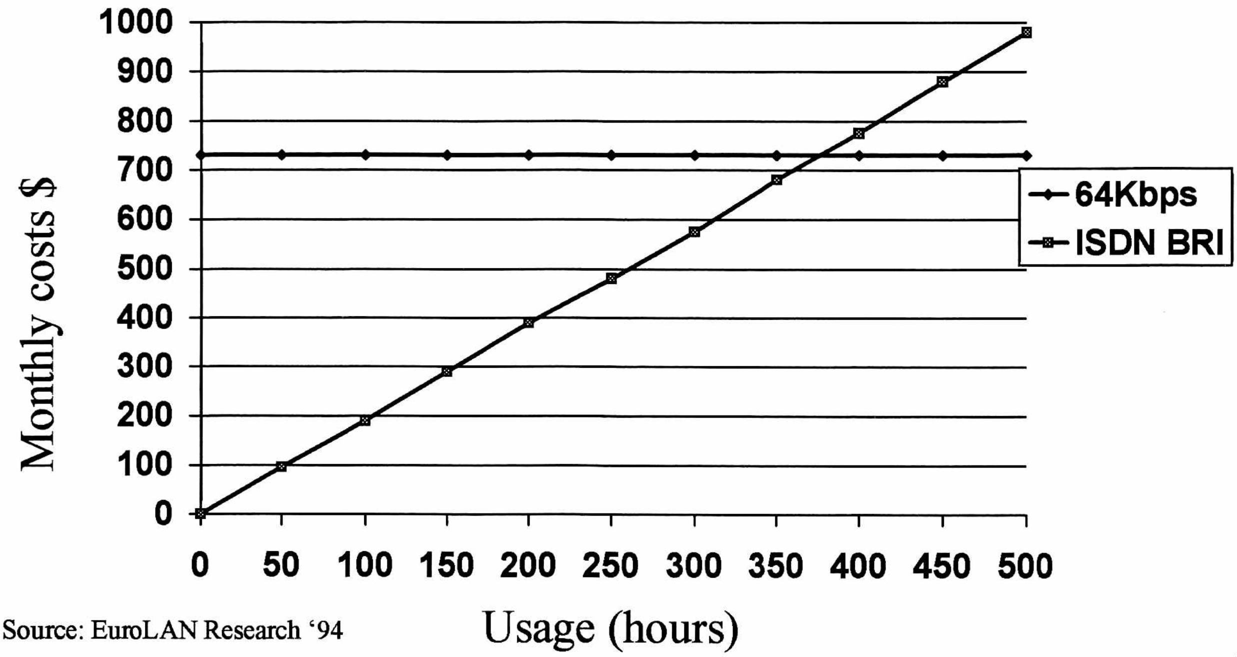
Internetwork Analysis and Troubleshooting, 10/96, Rev. 5.0

Network General

This graph represents a 10Km 64Kbps leased line cost compared to a single ISDN Basic Rate Interface line cost in France.

Usage of ISDN for local connections in France is cost beneficial over leased lines; up to 400 hours usage a month before ISDN costs equal leased line costs.

Leased Lines vs. ISDN BRI *Monthly Costs in Germany*

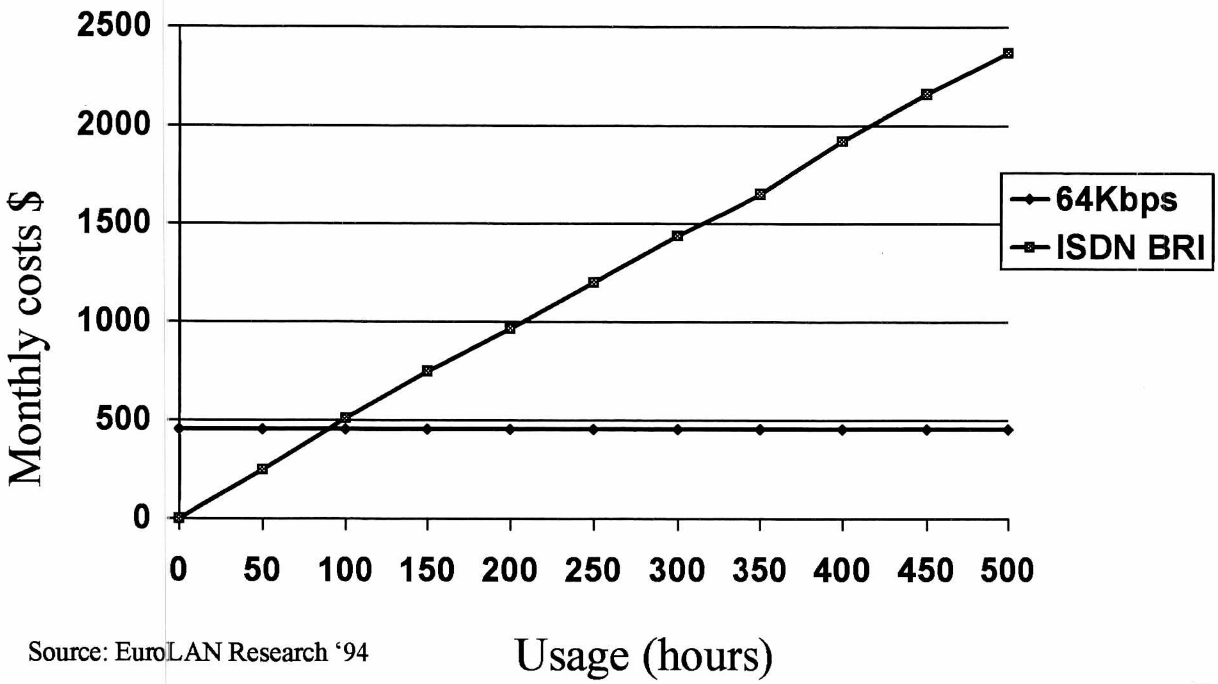


Source: EuroLAN Research '94

This graph represents a 10Km 64Kbps leased line cost compared to a single ISDN Basic Rate Interface line cost in Germany.

Germany has the most expensive leased lines. It also has the lowest cost benefit cut off point of 370 hours a month.

Leased Lines vs. ISDN BRI *Monthly Costs in the U.K.*



Source: EuroLAN Research '94

This graph represents a 10Km 64Kbps leased line cost compared to a single ISDN Basic Rate Interface line cost in the U.K.

The U.K. demonstrates a striking difference from both France and Germany. The low leased line costs (half those of Germany) and higher ISDN tariffs for local calls results in a low cost benefit cut off point (80 hours a month).

Different Countries
Different ISDN Signaling

	ISDN D Channel Signaling Protocol	ISDN Switch	Carrier / PTT
Germany	1TR6	Siemens	Deutsche Telekom
France	VN2	Alcatel	France Telecom
U.K.	ISDN2	AT&T	British Telecom Mercury Comm.

Every European country has their own national dialect of the ISDN D channel signaling messages. This means the ISDN switch located at the PTT supports a proprietary Layer 3 protocol that is based on the Q.931 protocol.

The differences between other national ISDN signaling protocols are slight, but the main differences between the national versions are the messaging formats.

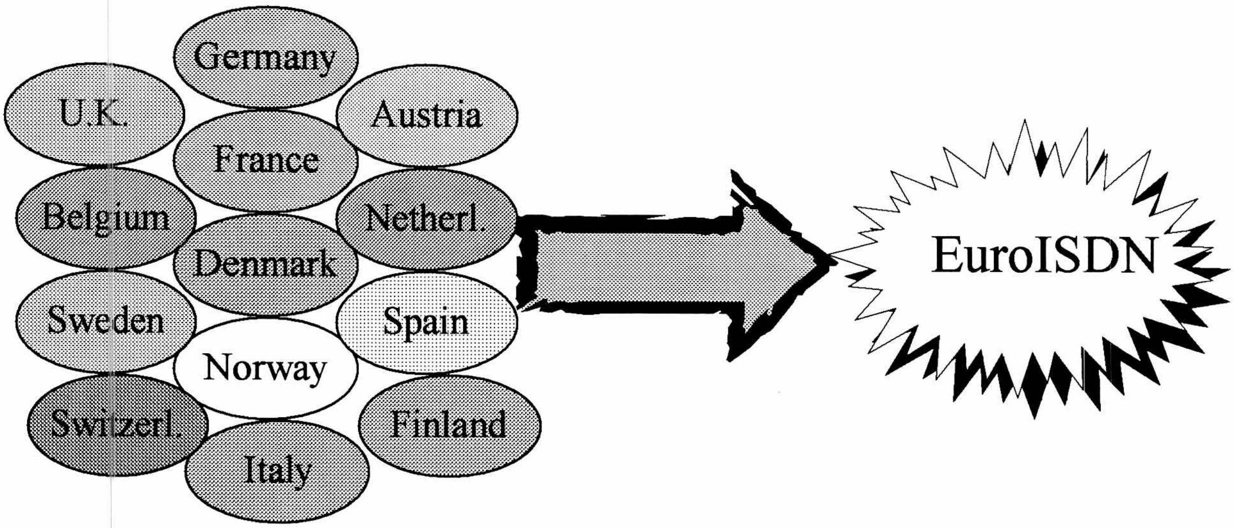
Proprietary ISDN switch protocols implement specific Layer 3 messages that, in most cases, pertain only to that countries' ISDN switches.

The specific messages for the different dialects often have to do with management of the subscriber's ISDN link. The user data still remains transparent and un-altered by the network.

These different dialects of the D channel call signaling means that ISDN equipment made in Germany, which support the 1TR6 signaling protocol, could not connect to an ISDN circuit in France, which support VN2.

As a result of the non-standard D channel implementation across Europe, user's ISDN equipment were confined to a specific country's national ISDN. This also introduced a new problem; ISDN D channel switch protocol incompatibility.

Different Countries
One ISDN Signaling Standard



SNIFFER® UNIVERSITY

Appendix 12 - 16

Internetwork Analysis and Troubleshooting, 10/96, Rev. 5.0

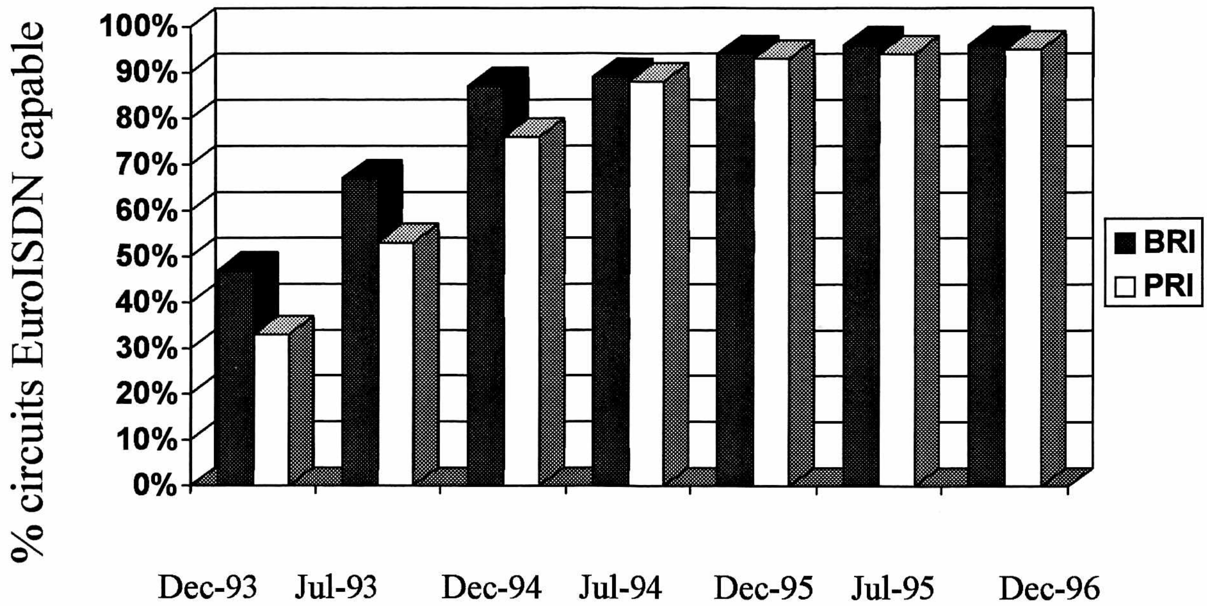
Network General

In 1989 carriers from 20 European countries signed an agreement to begin deploying EuroISDN.

EuroISDN comprises more than 200 specifications that define how European PTT's should implement ISDN services in their networks and how these services will be accessed by users.

At the end of 1993, 26 operators staged the European ISDN Event or "Eurie" to showcase the 1989 pacts to jointly implement EuroISDN specifications. Eurie gave European carriers an agreed set of services and network implementations to work towards.

European EuroISDN Service *Deployment*



Source: Ovum Research, '94

Availability of ISDN in France, Germany, and the U.K. has been 100% for several years, but many of the facilities were non-standard and country-specific.

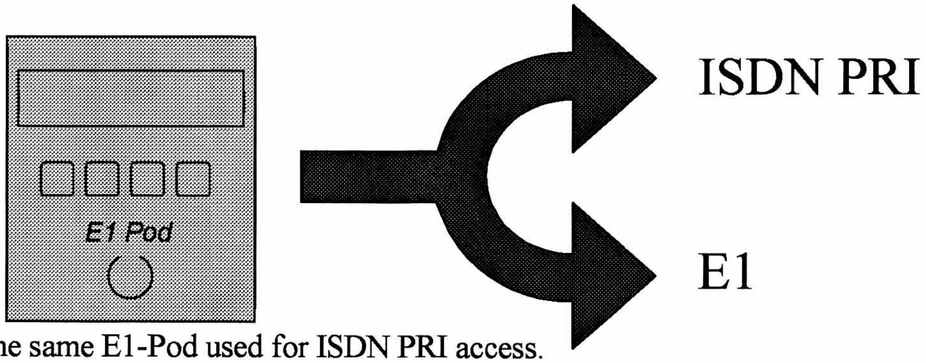
By the end of 1995 EuroISDN is expected to be 99% implemented in Europe (Ovum Research).

EuroISDN's Evolution

- Nearly all European PPTs support the EuroISDN standard for BRI and PRI.
- Some countries are still using their national ISDN signaling in addition to EuroISDN.
- EuroISDN will continue to be deployed by all European PTTs.
- By the end of 1995 EuroISDN is expected to be 99% implemented in Europe.

Existing E1-Pod is Used to Connect to a PRI

Using the existing E1-Pod customers it preserves your original investment. The E1-Pod can also be used for fractional or full E1 circuits.



The same E1-Pod used for ISDN PRI access.

LM2000

Objectives

On completion of this section you will be able to:

- Use the LM2000's features
- Check the LM2000's operation
- Perform physical layer testing
  - Break-out Box
  - BERT
- Insert and test the T-Pod Interface

Product Overview

- The LM2000 provides BERT, BLERT and physical interface testing to enhance LAN analysis.
- **Interfaces** - same as ESIA (RS-232, V.35, RS 449, V.10/11).
- **BERT and Break Out Box.**
- **Speeds** - 50 bps to 2.048 Mbps.
- Layers 1, 2, and 3 Analysis.
- **Protocol Decodes** - Frame Relay, ISDN, SNA, X.25, Async, Bisync.
- **PowerScript Test Builder** - allows creation of automated test routines.

The Main Menu

```
LM2000                          NETWORK GENERAL CORP.         Version num:      2.22
Protocol Analyzer                                             Serial # 00006502379E

              F1  Configure communications line
              F2  Automatically configure and start monitoring comm line
              F3  Monitor communications line
              F4  View monitored or captured data
              F5  BERT   Bit and Block error rate test
              F6  Break-Out box with pulse detection
              F8  PowerScript  Interactive test builder
              F9  Traffic generator     p

          ALT F1  Context sensitive HELP (from any screen)
        SHIFT F1  Read me
        SHIFT F2  Hardware configuration
        SHIFT F8  Async Terminal

        SHIFT F10 Exit High Speed Protocol Analyzer

    Note: Pressing the Shift key from any screen will show additional options

1CONFIG 2AUTO C 3MONITR 4VW BUF 5BERT   6BO BOX 7       8PSCRPT 9       10
```

Overview of Main Menu

Function Key	Label	Description
F1	CONFIG	System configuration Screen lets you determine interface board settings, define traps, configure capture options.
Alt F1	HELP	Context Sensitive Help.
F2	AUTO	Automatic Configuration automatically sets system config.
<Shift F2>	HW CONF	Hardware Configuration Screen.
F3	MON	Monitor Screen Displays during capture.
F4	VIEW	View Buffer displays data from the capture buffer.
F5	BERT	Bit/Block Error Rate Test Screen.
F6	BO BOX	Software Breakout Box.
F8	PSCRPT	PowerScript Custom Test Builder.
<Shift F8>	TERM	Async Terminal Emulator.
<Shift F10>	EXIT	Exit the LM2000 and return to DOS.


```
LM2000                        NETWORK GENERAL CORP.              Version num:     2.10
Protocol Analyzer                                                Serial # 0000650231C8

              F1  Configure communications line
              F2  Automatically configure and start monitoring comm line
              F3  Monitor communications line
              F4  View monitored or captured data
              F5  BERT   Bit and Block error rate test
              F6  Break-Out box with pulse detection
              F8  PowerScript  Interactive test builder


          ALT F1  Context sensitive HELP (from any screen)
        SHIFT F1  Read me
        SHIFT F2  Hardware configuration
        SHIFT F8  Async Terminal

        SHIFT F10 Exit High Speed Protocol Analyzer


1CONFIG 2AUTO C 3MONITR 4VW BUF 5BERT  6BO BOX 7      8PSCRPT 9      10
```

Checking the LM2000's Operation

Once the LM2000 hardware installation has been verified, verify the software installation by performing an emulation test using the common FOX message.

Make sure the LM2000 is not connected to a live network while conducting the test.

The FOX message is: A QUICK BROWN FOX JUMPED OVER THE LAZY DOGS BACK 0123456789...

The Fox Test

1) From the Main Menu, press **F3** to access the Monitor Screen. Then, from the Monitor Screen, press **F6 [CONFIG]** to access the System Configuration Screen.
2) Press **F4** [**MISC**] to change the **Emulation** from **DTE** to **DCE**.
3) At the System Configuration Screen, press **F7 [FOX]**. This loads the Quick Brown Fox test message. The message "FOX test configured" appears in the lower left corner of the screen.
4) Press **F10 [EXIT]** and **Enter** to save the Fox settings.
5) At the Monitor Screen, press **F1 [SYSTEM]** to enable the LM2000 (ensure the **SYSTEM** field says **RUN**).
6) Press **F4 [EMULAT]** to begin the FOX test.

If the FOX test succeeds, you will see the FOX message appear on the screen. The installation is complete and you are ready to begin data collection and analysis.

The following pages are screen shots you will see as a result of the above steps.

The FOX Test Lab Screen 1

```
LM2000                       NETWORK GENERAL CORP.              Version num:     2.22
Protocol Analyzer                                               Serial # 00006502379E

              F1  Configure communications line
              F2  Automatically configure and start monitoring comm line
              F3  Monitor communications line
              F4  View monitored or captured data
              F5  BERT   Bit and Block error rate test
              F6  Break-Out box with pulse detection
              F8  PowerScript  Interactive test builder
              F9  Traffic generator

          ALT F1  Context sensitive HELP (from any screen)
        SHIFT F1  Read me
        SHIFT F2  Hardware configuration
        SHIFT F8  Async Terminal

        SHIFT F10 Exit High Speed Protocol Analyzer

    Note: Pressing the Shift key from any screen will show additional options

1CONFIG 2AUTO C 3MONITR 4VW BUF 5BERT   6BO BOX 7       8PSCRPT 9       10
```

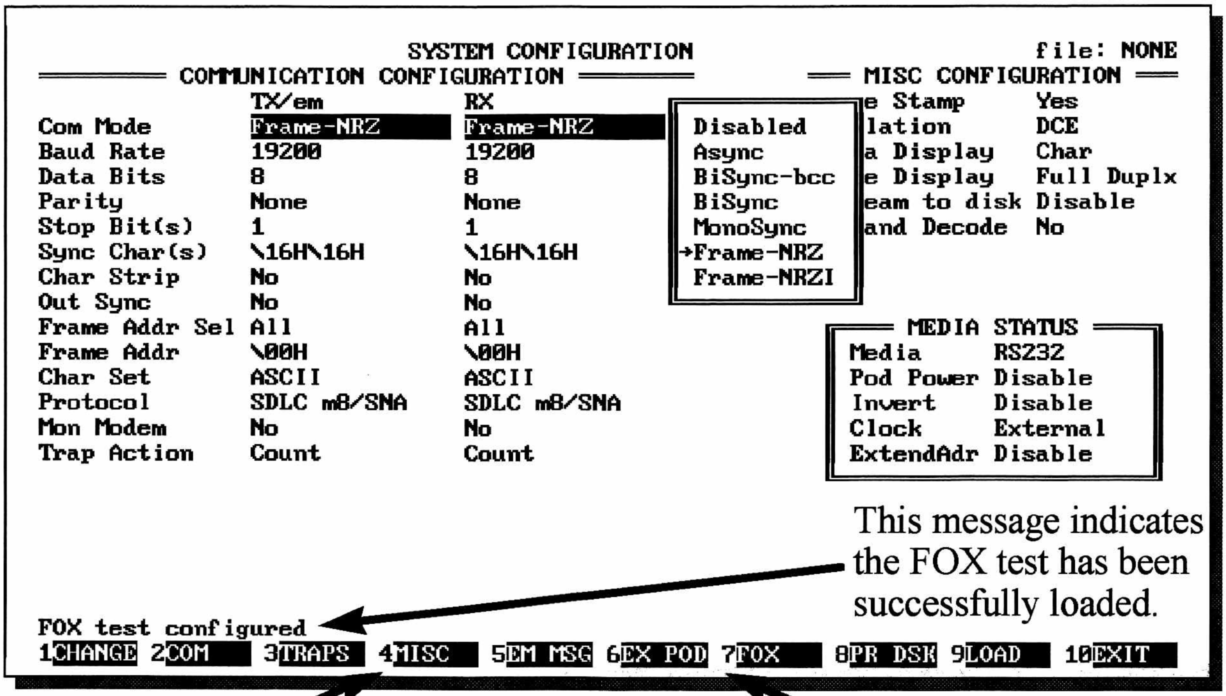
Press **F3** to access the Monitor Screen

The FOX Test Lab Screen 2

```
TX:↓ chrs:0          errors: 0      trap: disabled     DTR:↓  RTS:↓  TC:↓
RX:↓ chrs:0          errors: 0      trap: disabled     DSR:↓  CTS:↓  RC:↓
SYSTEM: RUN          screen: enabled buffer: enabled    emul:    disabled
                                    disk:    disabled
1SYSTEM 2SCREEN 3       4EMULAT 5VW BUF 6CONFIG 7SNAP S 8PR DSK 9STATUS 10EXIT
```

Press **F6** to access the System Configuration Screen

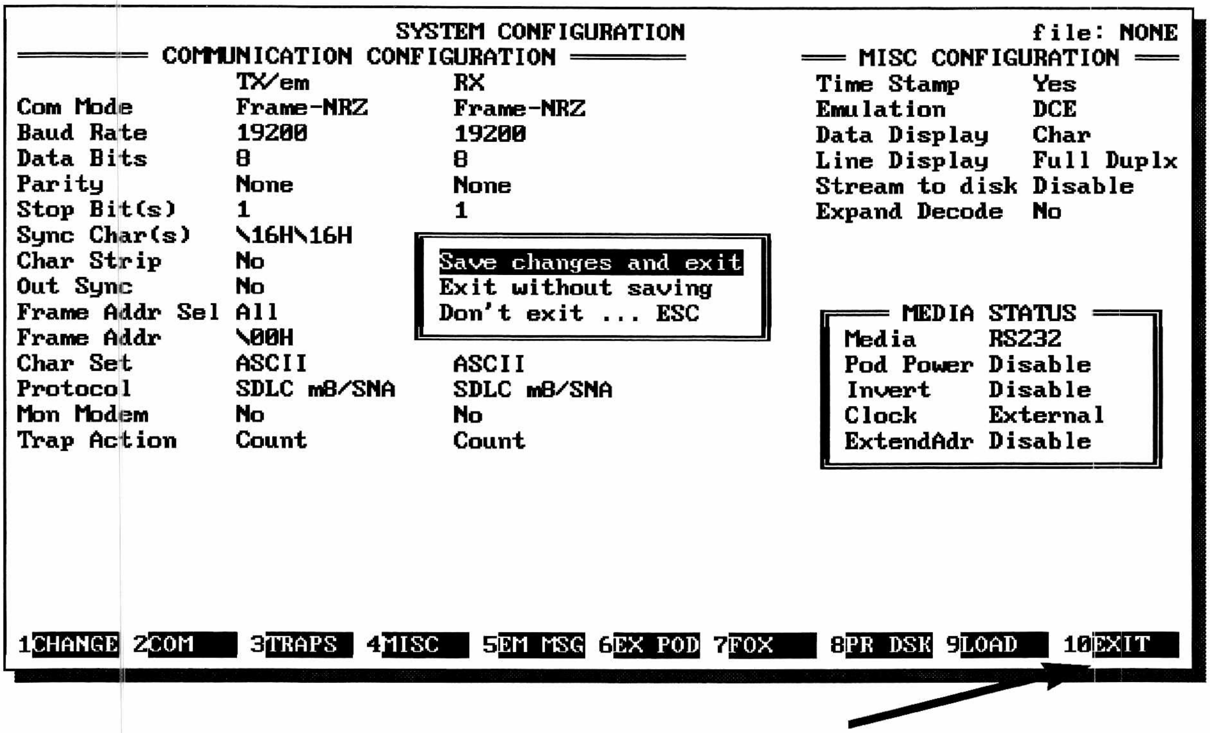
The FOX Test Lab Screen 3



1) Press **F4** to change the Emulation from DTE to DCE.

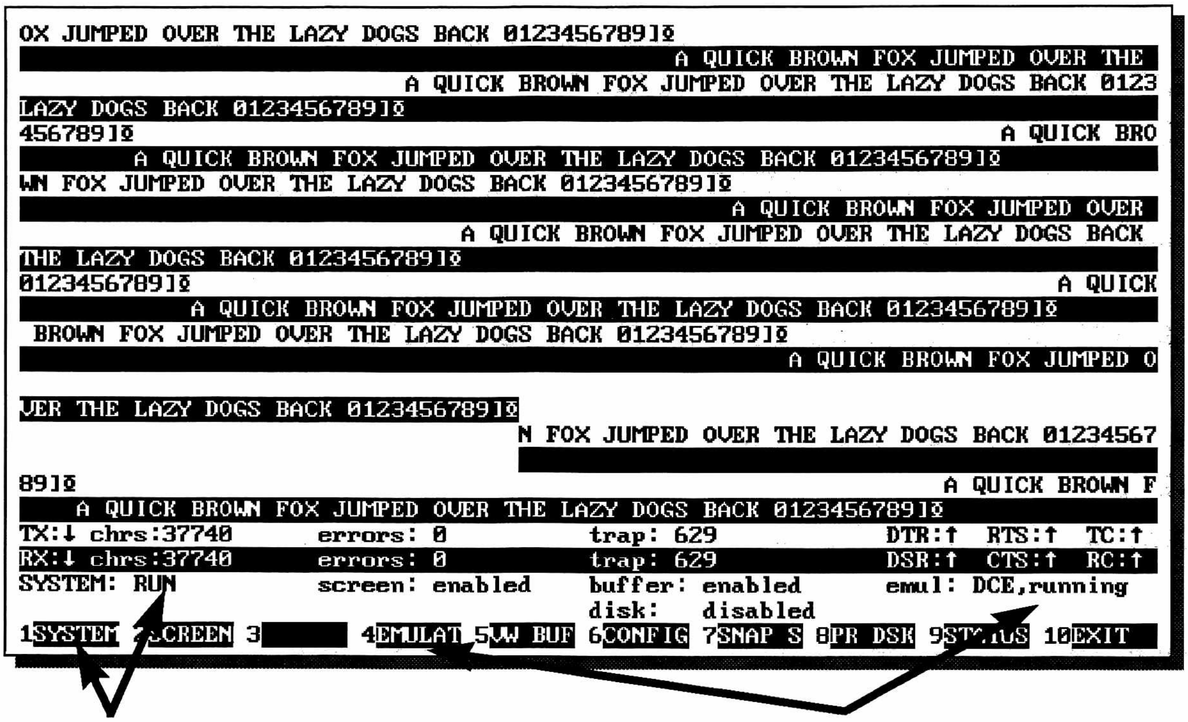
2) Press **F7** to load the LM2000 for the FOX test.

The FOX Test Lab Screen 4



Press **F10** to exit, and **Enter** to save the changes.

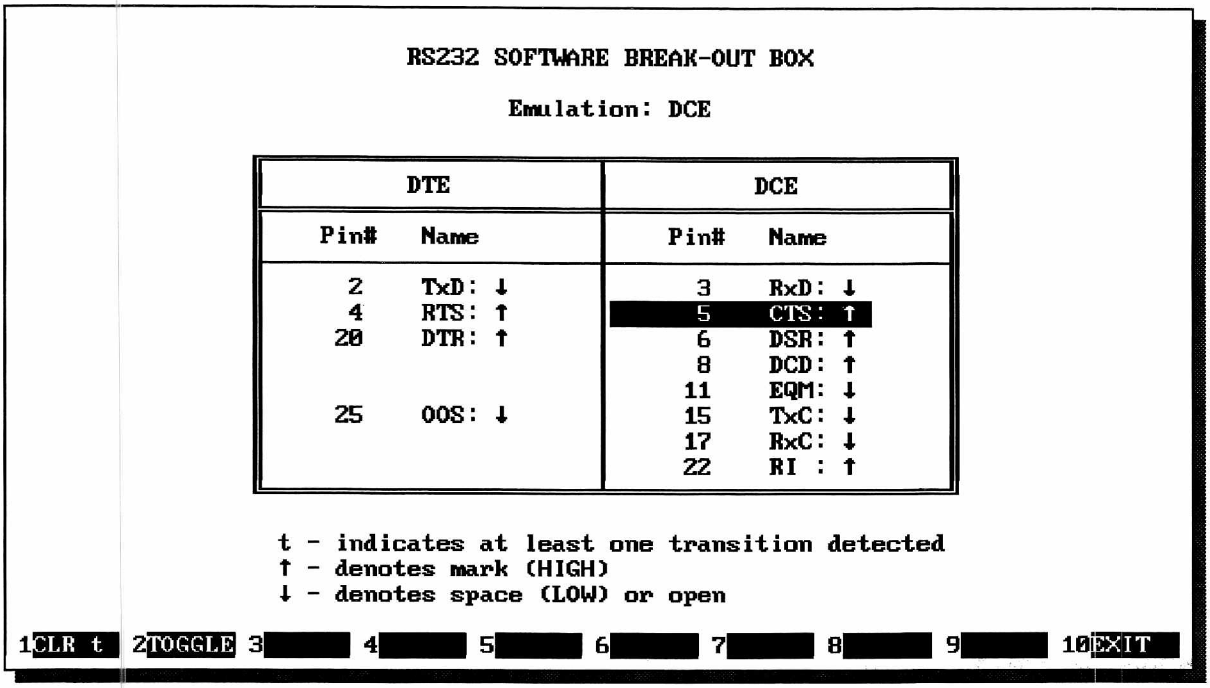
The FOX Test Lab Screen 5



1) Press **F1**; the System field says RUN.

2) Press **F4** to begin emulation; the EMUL screen says DCE running.

Software Break-Out Box Lab



SNIFFER® UNIVERSITY

Appendix 12 - 32

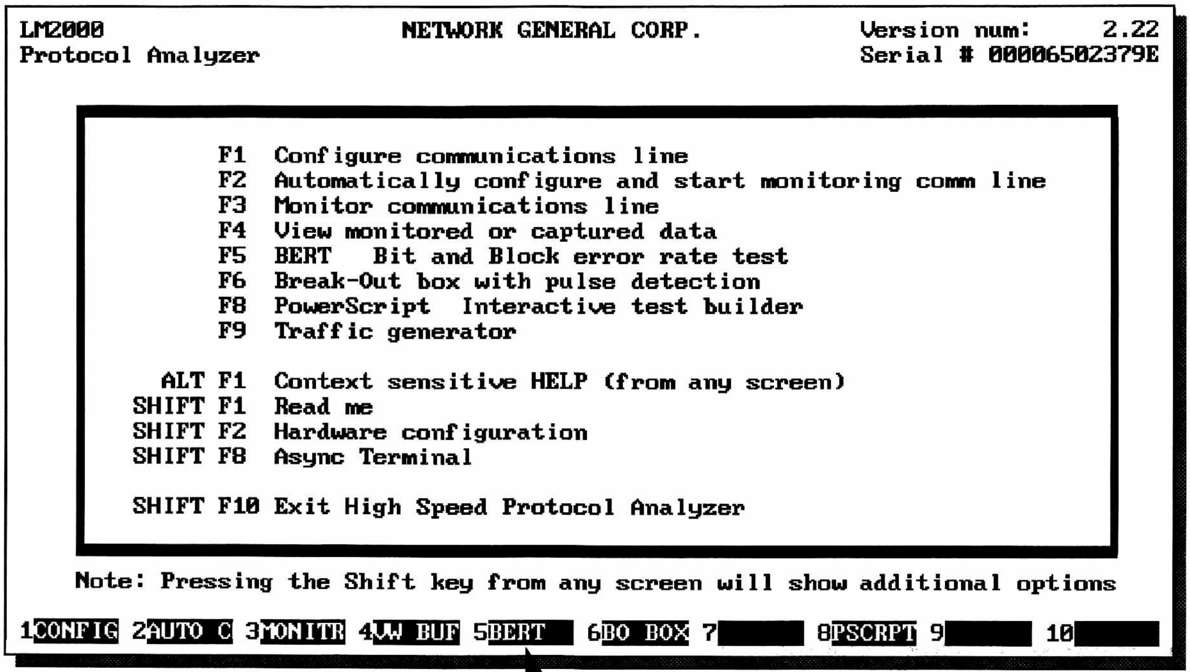
Internetwork Analysis and Troubleshooting, 10/96, Rev. 5.0

Network General

1. While still running the Fox Test, from the Monitor Screen Press **<Shift> F3** for the Break-Out Box.

Note: For a DCE emulation, the DSR and CTS leads are set high. In Addition, the Receive Data, Transmit Clock and Receive Clock leads are transitioning rapidly.

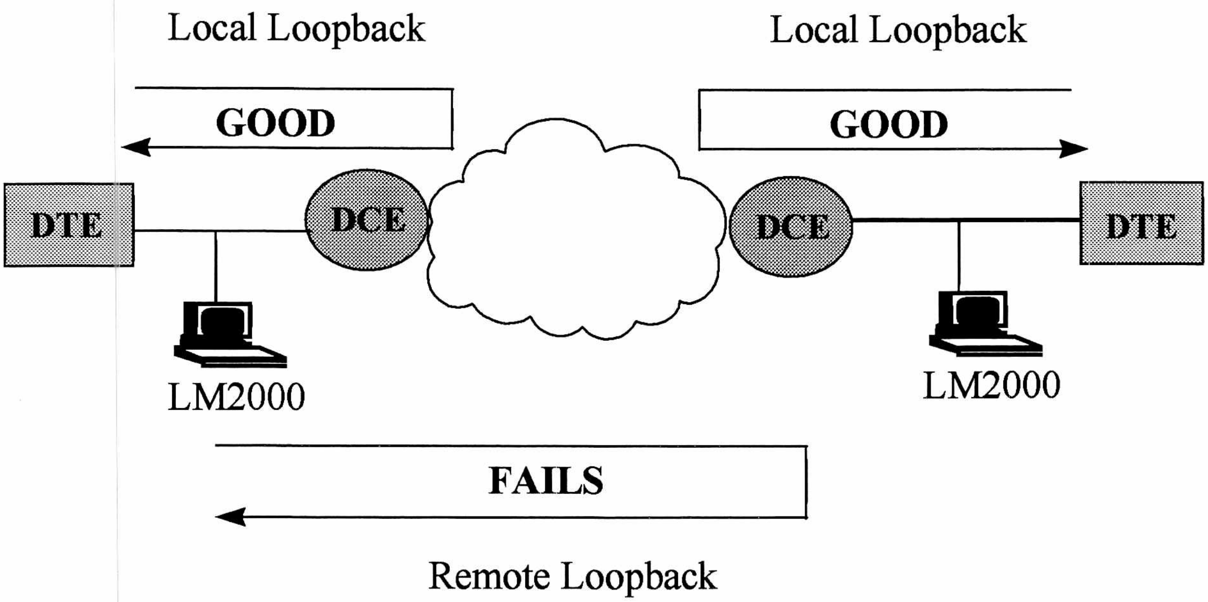
Bit/Block Error Rate Tests



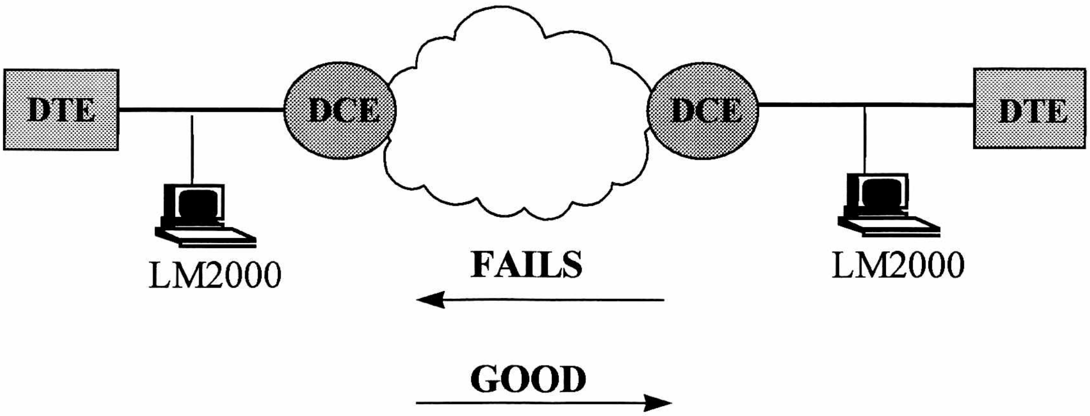
BERT/BLERT provides physical layer testing.

A BERT tests the quality of the line and is useful for proving to yourself or the phone company you are or are not getting what you paid for.

Using BERT to Isolate the Problem

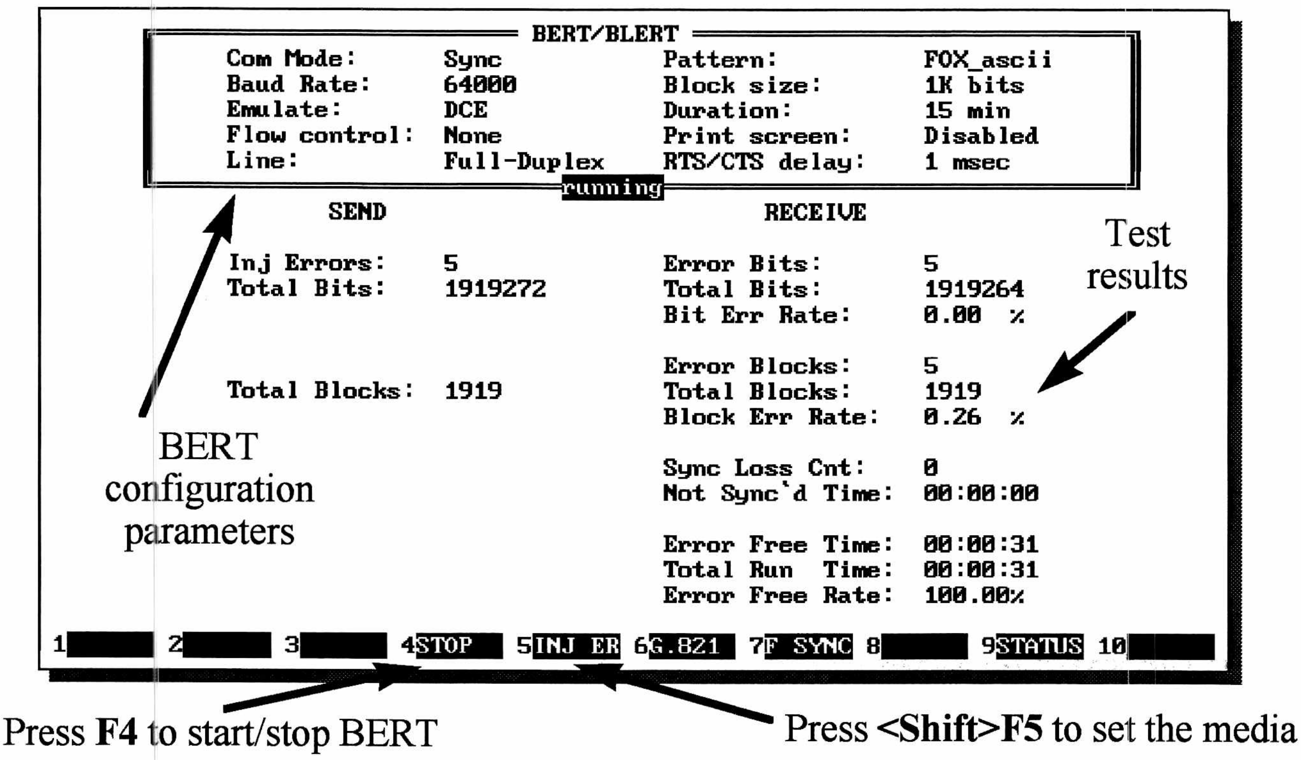


Using BERT to Isolate the Direction of Failure (End-to-End Test)



Appendix 12 - 35

Configuring BERT



SNIFFER® UNIVERSITY

Appendix 12 - 36

Internetwork Analysis and Troubleshooting, 10/96, Rev. 5.0

Network General

Emulate Specifies on which line emulation is to occur.

DCE Causes data transmissions to occur on pin 3. Modem leads DCD, DSR, and CTS are set high. LM2000 provides Tx and Rx clocks (pins 15 and 17 on RS232; pins Y, AA, and V,X on V.35) if a synchronous line.

DTE Causes data transmission to occur on pin 2. Modem leads DTR and RTS are set high. If a synchronous line, clocking is expected on pins 15 and 17 for RS232, and pins Y, AA and V, X on V.35.

Local Loopback BERT Lab

1. From the LM2000 Analyzer Main Menu, press **F5 [BERT]**. Press **Enter** on **Com Mode:** and arrow down to **Sync** and press **Enter**.
2. Change the **Emulate** to **DCE**. (On a loopback, the LM2000 Analyzer needs to be set to DCE but in the real world, it will be set to DTE).
3. Jumper pins 2 and 3 (Tx and Rx) on the DB-25 interface of the EISA card. Doing this loops back the transmitted data on to the receive line.
4. Press **F4** to start the BERT. Verify you are sending and receiving error-free bits.
5. Once you prove the local loopback is good on both sides of the network, you know the problem lies somewhere in between. The next step would be to perform a remote loopback. If for some reason the remote side cannot perform a local loopback, you can determine your side is good by performing a successful local and remote loopback.

SNIFFER® UNIVERSITY

Appendix 12 - 37

Internetwork Analysis and Troubleshooting, 10/96, Rev. 5.0

Network General

Many CSU/DSUs allow you to configure them for remote loopback across the network.

Understanding Error Results

Bit Error Rate - The ratio of error bits to total bits received. Most accurate of the three measurement tests.

Block Error Rate - The ratio of block errors to total blocks received. AT&T and the North American area define a block as 1000 bits.

Error Free Rate - The ratio of error free time to total time (in seconds). The second in which an error is detected is considered bad.

```
BLERT
     Pattern:              FOX_ascii
     Block size:           1K bits
     Duration:             15 min
     Print screen:         Disabled
     RTS/CTS delay:        1 msec
ning
                 RECEIVE

     Error Bits:           0
     Total Bits:           67601592
     Bit Err Rate:         0.00  %

     Error Blocks:         0
     Total Blocks:         67601
     Block Err Rate:       0.00  %

     Sync Loss Cnt:        0
     Not Sync'd Time:      00:00:00

     Error Free Time:      00:00:34
     Total Run  Time:      00:00:34
     Error Free Rate:      100.00%

B 6G.821  7F SYNC 8       9STATUS 10
```

The BERT should be run for at least 15 minutes.

SNIFFER® UNIVERSITY

Appendix 12 - 38

Internetwork Analysis and Troubleshooting, 10/96, Rev. 5.0

Network General

"No data" is not considered an error. In other words, if the LM2000 analyzer loses sync the **Not Sync'd Time** would increase as well as the **Error Free Time.** If the **Error Free Rate** was 100.00% prior to losing sync, it would remain 100.00% after losing sync.

F6 Key labeled G.821 changes the screen to the universal format.

Analyzing BERT/BLERT Results

```
==================== BERT/BLERT ====================
 Com Mode:        Async-8        Pattern:          FOX_ascii
 Baud Rate:       19200          Block size:       1K bits
 Emulate:         DCE            Duration:         15 min
 Flow control:    None           Print screen:     Disabled
 Line:            Full-Duplex    RTS/CTS delay:    1 msec
=====================running========================
        SEND                             RECEIVE

 Inj Errors:      5              Error Bits:       5
 Total Bits:      153552         Total Bits:       153552
                                 Bit Err Rate:     0.00  %

                                 Error Blocks:     5
 Total Blocks:    153            Total Blocks:     153
                                 Block Err Rate:   3.27  %

                                 Sync Loss Cnt:    0
                                 Not Sync'd Time:  00:00:00

                                 Error Free Time:  00:00:11
                                 Total Run  Time:  00:00:11
                                 Error Free Rate:  100.00%

1      2      3      4STOP   5INJ ER  6G.821  7      8      9STATUS  10
```

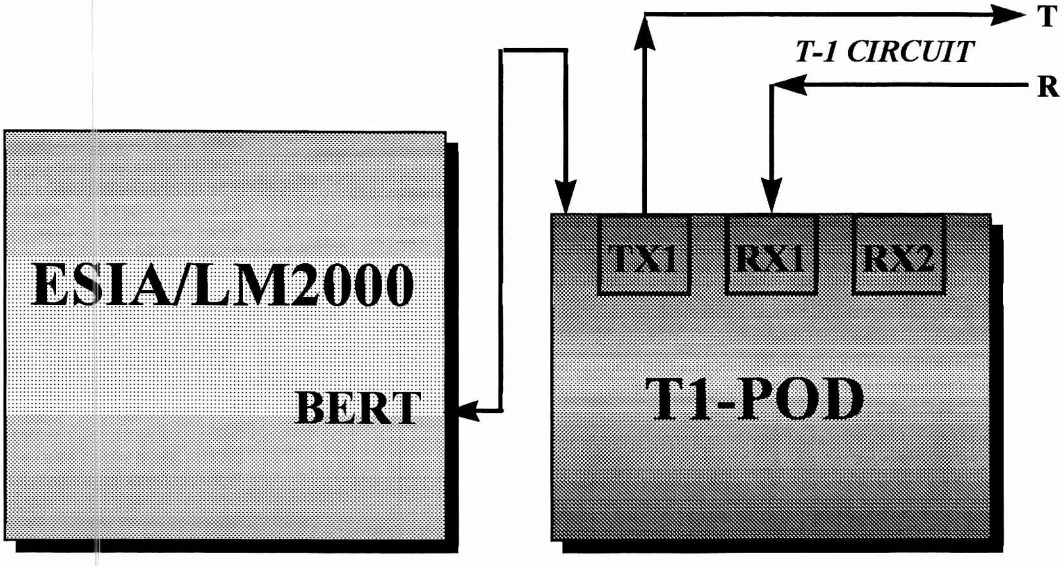

Some not so obvious fields are:

Error Blocks Number of blocks received with at least one error.

Sync Loss Cnt Number of times the LM2000 re-synched on the received data stream either automatically (due to abnormally high bit rate) or forced resynchronization (you press F7).

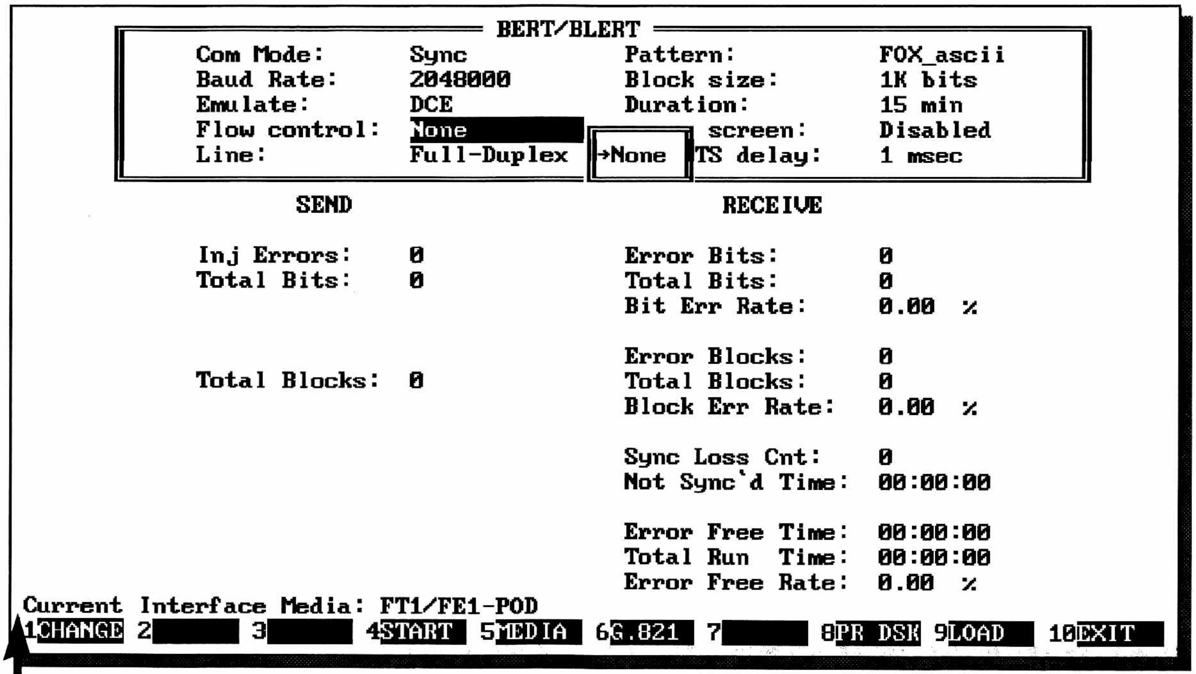
Not Synch'd Time Number of seconds the received data stream was not synchronized.

Putting It All Together: BER Testing T-1 with the T1-POD



The T-1 Pod can be configured to access any or all 24 DS-0s in a T-1 circuit. A BERT can then be run on the ESIA/LM2000 through the T-1 Pod to verify the T-1 physical integrity.

T1-Pod BERT Loopback Demo



Fractional T-1 pod selected

1. Connect the FTPOD to the LM2000 DB15 port, and load the LM2000 Analyzer.

2. Select F1 [Configure Communications Line]
   Select F6 [EX POD], exit and save.

3. Select F5 [BERT] from the main menu:

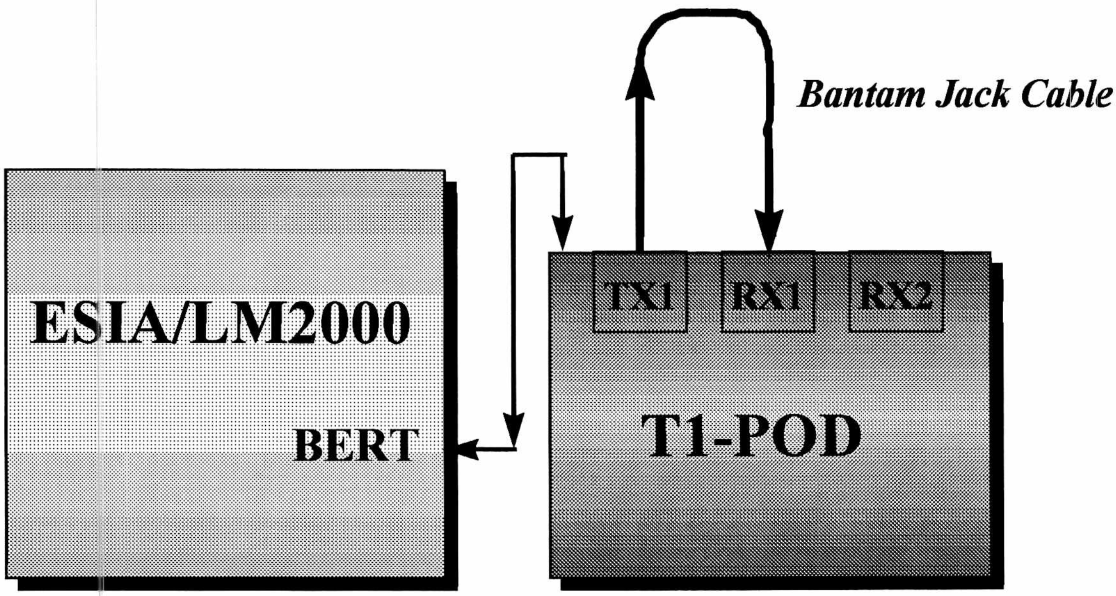
   Select Com Mode: **Sync**
   Set Baud Rate: **1536K** (T-1 rate)
   Emulate: **DTE**
   Flow Control: **none**

4. Select F5 [Media]: Select **FT1-POD**

Press <ESC> to return to main screen

T1-Pod BERT Demo

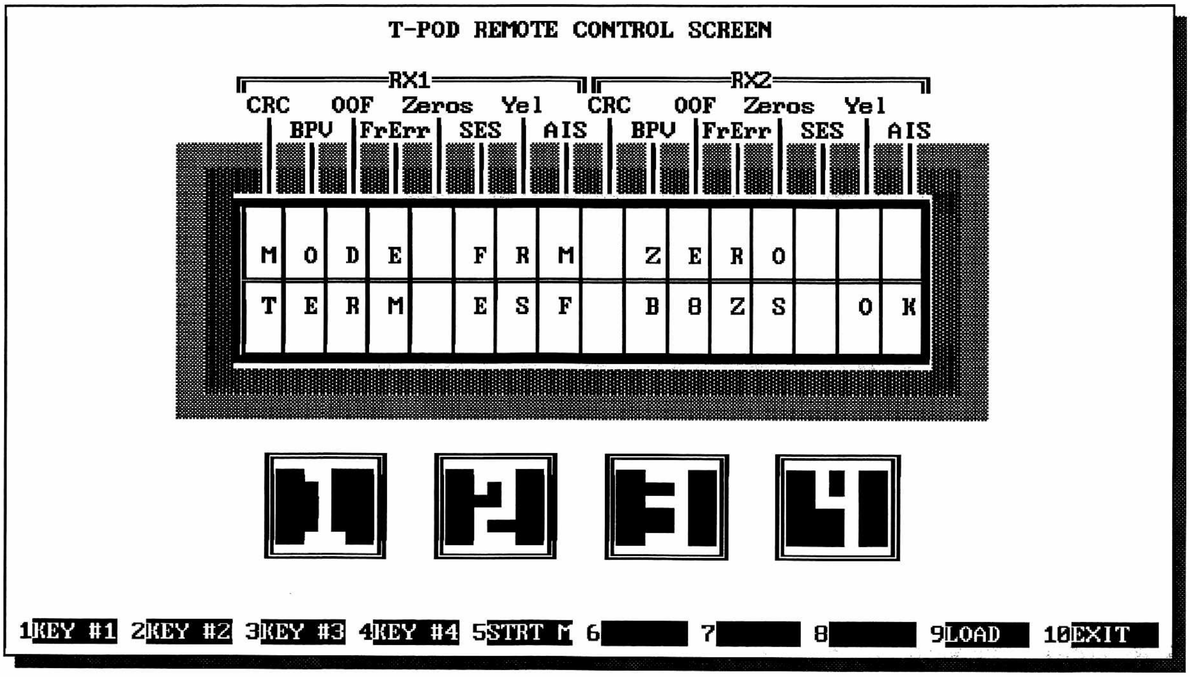
Continued



Place a loopback from TX1 to RX1 on the T-Pod, using a Bantam Jack cable.

T1-Pod BERT Demo

Continued



5. Press F6 [BO BOX] from the main screen
   Program the T-POD as follows:
   Press F1 [SET]

   Select MODE: **TERM**
   Select FRM: **ESF**
   Select ZERO: **B8ZS**

   Press F4 [OK]

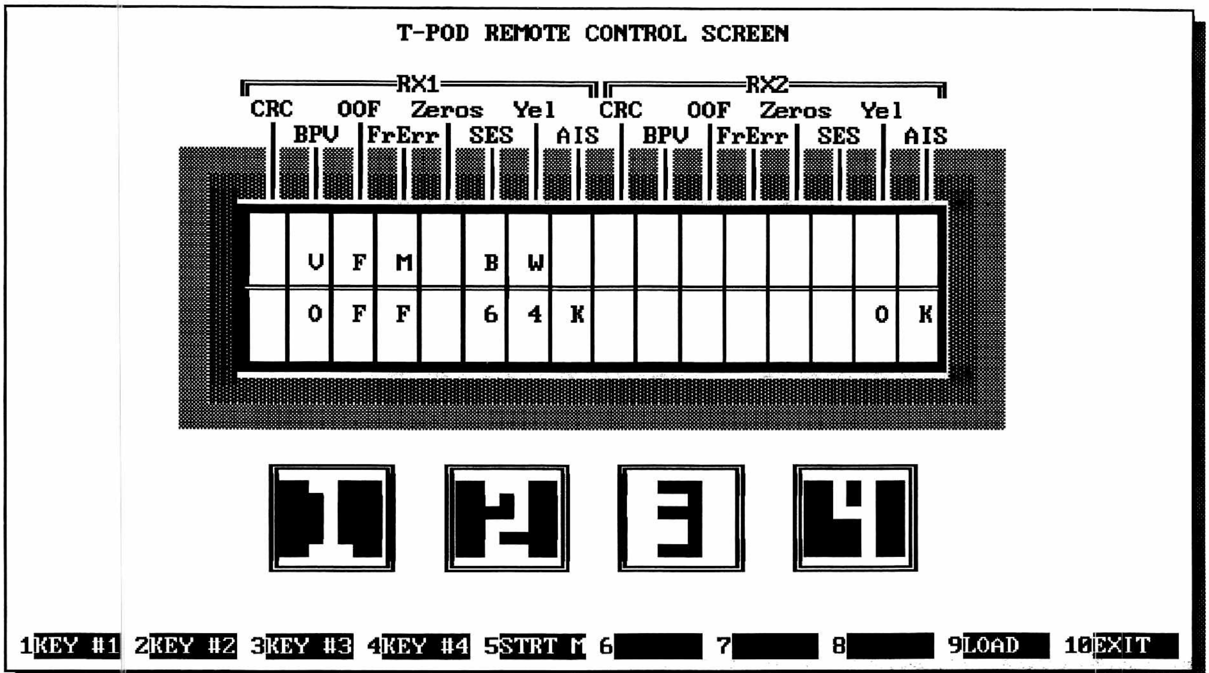
TERM -Terminate test mode. Allows protocol analyzer to monitor incoming data on RX1 while transmitting test data on TX1.

ESF - Extended Super Frame. Consists of 24 193 bit frames. Incorporates a CRC, and datalink channel for sending status messages between both ends of the T-1 link.

B8ZS - Bipolar with 8 Zero Substitution. A means of coding long strings of zero bit transmissions to maintain circuit timing parameters.

T1-Pod BERT Demo

Continued



6. Select CLOCK: **MASTER**
   Press F4 [OK]

   Select VFM: **OFF**
   Press F4 [OK]

   Select BW: **64K**
   Press F4 [OK]

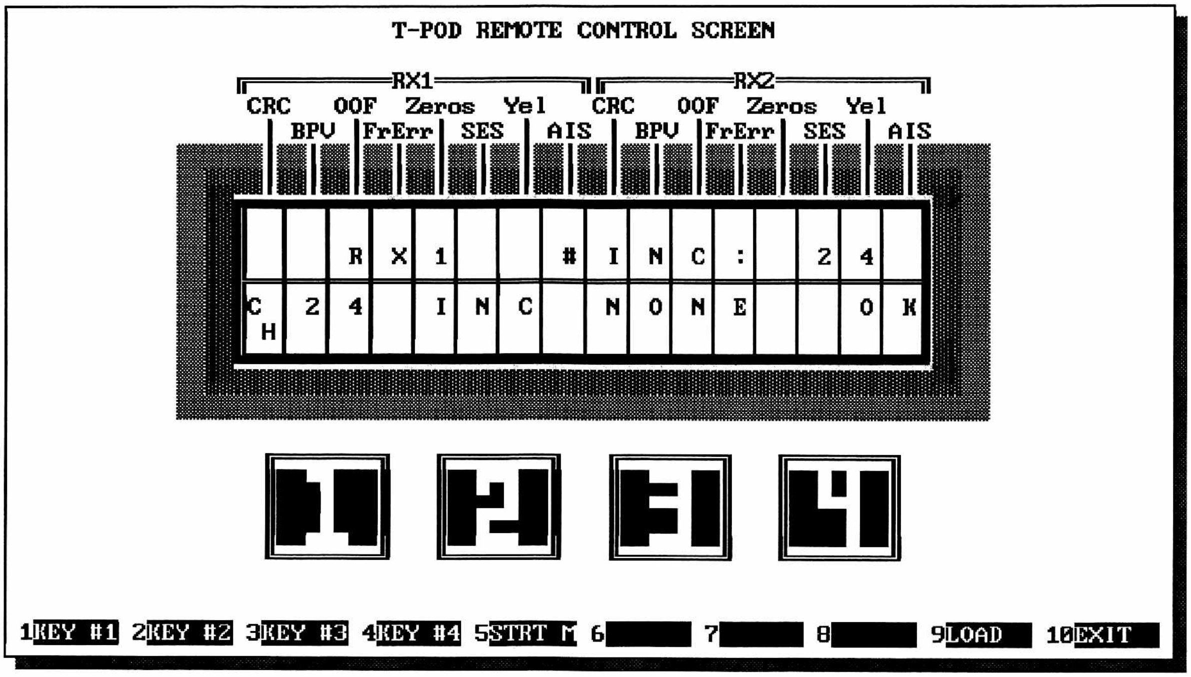
MASTER CLOCK - T-Pod provides clocking to the T-1 circuit.

VFM OFF - Turn off Voice Frequency Monitor.

BW 64K - Each channel will have 64K bandwidth.

T1-Pod BERT Demo

Continued



7. Verify: **RX1 # INC: 24**
   Press F4 [OK]

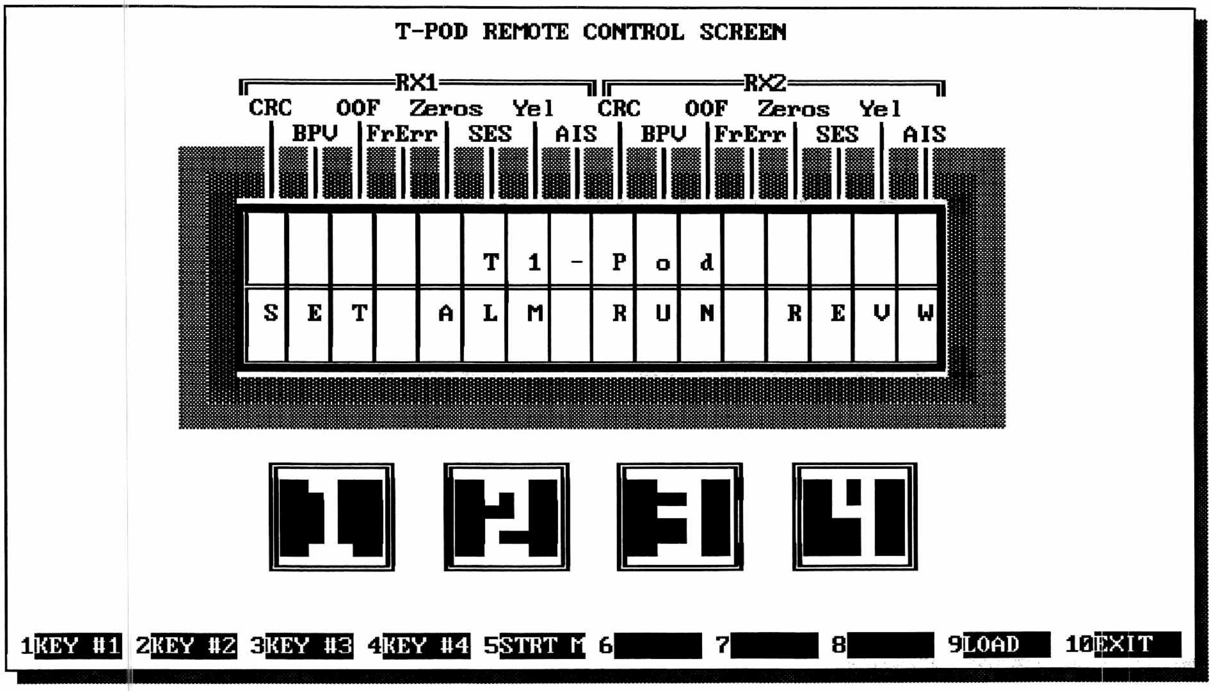
   Verify: **COPY RX1 TO RX2?**
   Press F4 [YES]

RX1 # INC: 24 - Selects all 24 channels in the T-1 for monitoring.

COPY RX1 TO RX2? - selects the same channels for RX2 as were selected for RX1.

T1-Pod BERT Demo

Continued



SNIFFER® UNIVERSITY

Appendix 12 - 46

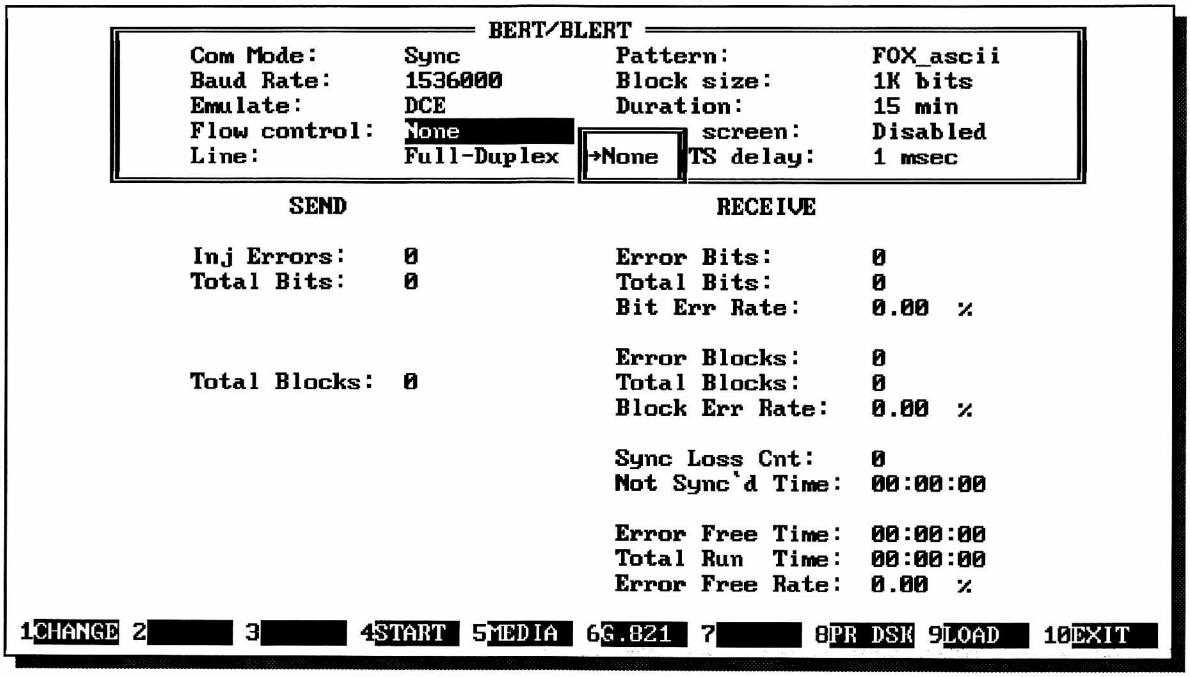
Internetwork Analysis and Troubleshooting, 10/96, Rev. 5.0

Network General

7. Press F3 **[RUN]**
   Press <ESC> to return to main screen.

T1-Pod BERT Demo

Continued



8. From main screen Press F5 **[BERT]**
   From BERT screen Press F4 **[START]** to start test

   Total Bits SEND and RECEIVE should match.

Summary

- The LM2000 provides BERT, BLERT and physical interface testing to enhance LAN analysis.
  - It provides the same interfaces as the ESIA.
  - BERT and a Break-out box testing available.
  - Tests 50-2.048 Mbps lines.
  - Decodes layers 1-3: Frame Relay, ISDN, SNA, X.25, Async and Bisync.
- The LM2000's operation can be tested with the FOX message.
- Physical layer testing can be done using a software Break-out Box or BERT.
- A T-Pod Interface allows you to insert into a T1 line to do BERT testing.

LAN/WAN Supplemental Exercises

Appendix 12 - 49

Protocol Forcing Exercise 1

Objective: To develop familiarity with Protocol Forcing LAN packets from within WAN frames.

Background: The trace file used is from a Frame Relay device that forwards both bridged and routed Ethernet LAN traffic over the WAN.

1. **Load** and **display** C:\SYCAP\TC107\FSFR01-R.SYC with **Detail** and **Hex** windows enabled. Press **F3** twice to display the data. Note the highest layer protocols decoded for the first 4 frames displayed in the Summary window.

2. **Tab** into the Detail window and **Home** to the top of frame 1. **Cursor down** to the end of the FRELAY header and the beginning of the IP header. Note that the last field in the FRELAY header is an Ethertype that points to the embedded upper layer protocol, IP.

3. These frames are typical of frames forwarded by a Frame Relay router. (The DLC addresses are not forwarded by the router on the WAN link as they are recreated by the router on the LAN.) Write down the 2-byte Ethertype associated with IP.

Protocol Forcing Exercise

Continued

4. Use **F8**, Next Frame, to navigate to frame 4 and write down the Ethertype for Novell IPX. Do there appear to be any other Ethertypes in this trace file? Notice that there are Frame Relay LMI management frames in the trace file. Use **Relative time** to determine the periodicity of the LMI Keep Alive Status frames.

5. Now **Load and Display** C:\SYCAP\TC107\FSFR01-B.SYC. Can the Sniffer Analyzer determine what the Ethertype is? How many bytes of FF are there at the beginning of the first embedded packet? If you combine these bytes with the next 6 bytes, and examine the next two bytes at offset 0E, is it possible that this is an Ethernet header?

6. Use **F6** for Display Options, **Protocol Forcing**. Set **Rule 2** so that "If Frame Relay", "Then Ethernet": press **Enter** on **If** and select **Frame Relay**; press **Enter** on **Then** and select **Ethernet**. Press **F3** to display the data.

Protocol Forcing Exercise

Continued

7. Examine frame 1. If the pattern at offset 0E is 8137, the Ethertype for Novell IPX, then the Sniffer should be displaying the first 26 frames as NetWare SAPs. (SAPs, Service Advertisement Protocol frames, are accumulated by the router and propagated to the next locally connected router every 60 seconds.)

8. The Ethertype at offset 0E in frame 27 should be 809B for AppleTalk and the Ethertype at offset 0E in frame 40 should be 0800 for IP. This should now appear to be Frame Relay bridged traffic instead of routed traffic. The Frame Relay device has encapsulated the entire Ethernet LAN frame in a Frame Relay WAN header.

9. Now that we have developed some experience with protocol forcing, let's try a trace file with both bridged and routed traffic in it. Use **Display Options**, **Protocol Forcing**, and **disable** Rule 2 using the **space bar** (x beside Rule 2). From the Main Menu, **load** and **display** the trace file C:\SYCAP\TC107\FSFR01.SYC.

Protocol Forcing Exercise

Continued

10. Frame 1 should be the same as in the first trace file, FSFR01-R.SYC we worked on earlier. Note that the expected Ethertype is 0800 (IP) at offset 02. Frame 30 has an Ethertype of 8137 (Novell IPX) at offset 02. These are routed frames. Frame 2 appears to be a bridged frame.

11. Let's setup a protocol force like the one we used earlier with one exception: we'll use Pattern Match in Rule 1 to Protocol Force all of the routed frames to their appropriate Ethertypes, and then we'll use Pattern Match in Rule 2 to Protocol force all of the remaining bridged Ethernet frames.

12. Highlight the Ethertype pattern of 0800 at offset 02 in frame 1. Use **F6** for Display Options, choose **Protocol Forcing,** then choose **Rule 1**. Press **Enter** on **If,** select **Frame Relay**, and press **Enter**. Cursor down to **Pattern Match**, cursor right and up to **Pattern**, press **Enter**, type **0800** or press the **up arrow**, press **Enter**, cursor down to **Offset=**, press **Enter**, type **02** or press the **up arrow** , press **Enter**, cursor left and down to **Then**, press **Enter**, cursor down to **Ethertype**, press **Enter**, then display the data with **F3**.

Protocol Forcing Exercise

Continued

13. In summary, we have setup Protocol Force Rule 1 so that if a Frame Relay header is encountered, then treat the pattern 0800 at offset 02 as an Ethertype.

14. Now use **F8** repeatedly to get to frame 30 and highlight the the Ethertype pattern of 8137 at offset 02. Use the lower half of the Pattern Match you worked on in question 11 (Rule 1) so that the **Pattern=8137** at **Offset=02**. Don't forget to change the logical operator from AND to <u>OR</u> by using **spacebar**.

15. In summary, we have setup Protocol Force Rule 1 so that if a Frame Relay header is encountered, then treat the pattern 0800 or the pattern 8137 at offset 02 as an Ethertype. This will "set the Ethertypes" of the routed frames. Press **F3** to display the frames. Now let's work on the bridged frames.

16. Use **F6** for Display Options, **Protocol Forcing**, **Rule 2** so that **If Frame Relay, Then Ethernet**. We did this earlier so we simply have to enable Rule 2 with **spacebar**. Display the trace file once again with **F3**.

Note: if you don't "set the Ethertypes" before telling Sniffer to treat the rest as bridged Ethernet frames, then Sniffer will treat them <u>all</u> as Ethernet frames.

Protocol Forcing Exercise

Continued

17. The remaining bridged frames should now be displayed correctly. There should be a Novell SAP in frame 2, a TCP packet in frame 28, AppleTalk NBP in frame 37, and a RIP in frame 459. Save this setup using **F5**, **Files**, **Save**, **Setups** as **FSFR01** - the same as the trace file name. We will examine the frames in more detail in the Frame Relay section.

WAN Troubleshooting Exercise

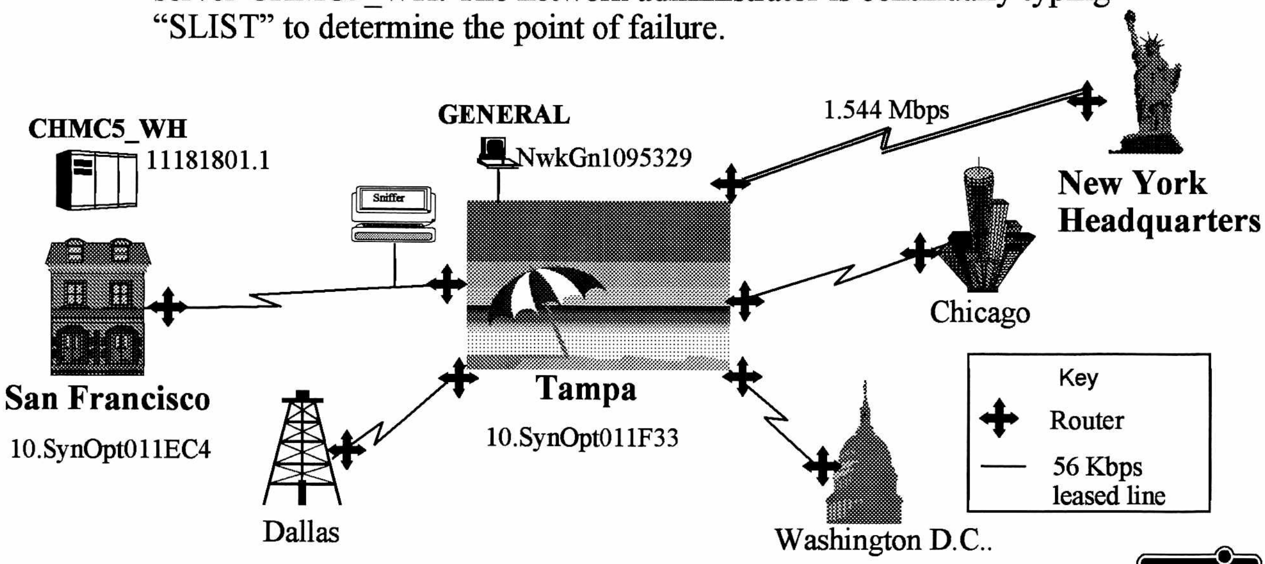
Objective: Troubleshoot a problem in a Novell NetWare wide area leased line environment.

Background: IPX routers use the Routing Information protocol (RIP) to broadcast their routing tables every 60 seconds. Other IPX routers listen to these broadcasts and update their tables accordingly. The Service Advertising protocol (SAP) allows Novell services such as file and print servers to advertise their services and network numbers. Through SAPs, IPX routers build and maintain a Server Information Table (SIT) or SAP table. Routers also broadcast their SAP tables every 60 seconds. When a Novell client wants to reach a server, gateway or printer, it can obtain the network address from a nearby router.

Problem: Remote users with sessions to Tampa are disconnected within minutes after the IPX router to New York is brought on line. Users at remote sites are not experiencing any disconnect problems communicating with Tampa when the IPX router is not connected to New York.

WAN Exercise (Cont'd)

Testing : An ESIA was setup to capture traffic between Tampa and San Francisco. Three tests were run: **PRETEST2.SYC** is captured data prior to turning on the router to NY; **TEST3.SYC** is captured data after turning on the router to NY; **TEST4.SYC** is captured data after the "fix." GENERAL, a test PC on network 1 operated by the network administrator, is attached to server CHMC5_WH. The network administrator is continually typing "SLIST" to determine the point of failure.



WAN Exercise

Continued

1. **Load** the file C:\SYCAP\TC107\PRETEST2.SYC. This is the capture prior to turning on the router to NY. A filter has been applied to filter out the SNMP frames from the router and display only NetWare traffic.
2. Display the **Expert Overview** screen. What is the diagnosis?

   Press **Enter** at the **Application Diagnosis Summary** screen. Press **Enter** once more to see that GENERAL and DENNISON are stations receiving a slow response from the remote server.
3. Press **Esc** until you get back to the **Expert Overview** screen. Since there are no diagnoses at the DLC Stations and Global Symptoms, could the slow server diagnosis be the result of a congested network?
4. Based on your answer to number three, what is your hypothesis about the cause of the network failures after the router was turned on? (Hint: use the "layered' approach to troubleshooting. We have ruled out the WAN link [layer 2] as the problem. What other layer could be responsible for catastrophic system wide failures?)

WAN Exercise

Continued

5. Display the data. Which frame marks the beginning of the first SAP table broadcast?

   Why do you think multiple SAPs were sent?

   Turn on your **Relative time** and **Cumulative bytes**. How long does it take 10.SynOpt011F33 to broadcast its SAP table?

   How many cumulative bytes?
6. Press **F6** for **Display options**. Move to **Manage names**, **Edit Names**. Give 10.SynOpt011F33 the name "Tampa_Router." Give 10.SynOpt011EC4 the name "Frisco_Router."
7. Display the data. Find the first occurrence of an IPX RIP packet. (Frame 35). How many networks does Tampa_Router advertise prior to enabling the router to NY?

WAN Exercise

Continued

8. Find the RIPs and SAPs from Frisco_Router. (Hint: **Search for text** on the word "RIP".) How many networks does this router advertise?

9. Novell recommends staggering RIP and SAP updates every 30 seconds so that the network and routers are not burdened with processing each simultaneously. Has the router vendor implemented that here?

   Novell also requires a minimum interpacket gap of 55 milliseconds between a series of SAP packets. Do both of these routers comply with this specification?

10. To find out if the routers are functioning correctly, press **F6** Display options to set up a Station address Filter Match 1 for Tampa_Router. Does it send RIPs and SAPs every 60 seconds as expected?

    Turn off that filter (press the spacebar next to **Match 1** to deselect it) and repeat the same process using **Match 2** to verify Frisco_Router is also operating normally.

WAN Exercise

Continued

11. **Load** C:\SYCAP\TC107\TEST3.SYC. This trace was captured after the NY router was turned on. What are the diagnoses?

    Press **Enter** on the **Connections layer diagnosis** until you get to the **Connection Detail** screen. Note that GENERAL was the station connected to CHMC5_WH during the non-responsive diagnosis.
12. You should still have a **Station address** filter set for Frisco_Router. Are the RIPs and SAPs normal compared to your benchmark; that is, do they each occur every 60 seconds?
13. Enable your **Station address** filter for Tampa_Router. We will examine the RIPs and SAPs to determine if anything has significantly changed since the pretest. What is the cumulative number of bytes sent and relative time of the first SAP table broadcast?

    Since the NY router has been turned on, how many networks is Tampa_Router advertising?

WAN Exercise

Continued

What is the time delay between the first and second RIP packets?

14. Examine the RIPs and look for any departures from the norm. Do you notice any?

15. Examine the SAP broadcasts. (You don't need to look in the **Detail** window for this; just examine the size, duration, and frequency to note differences from the pretest.)
16. Remembering that GENERAL was on network 1 when the SIA diagnosed CHMC5_WH as non-responsive, examine the **Detail** window of the partial RIP packets (3690, 4687, and 5678) and develop a hypothesis about the cause. (Hint: routers implement an aging mechanism whereby table entries are deleted if an update containing that table entry has not been received in three minutes).

WAN Exercise

Continued

17. What might you do to fix this problem?

18. If interested you may **load** the file C:\SYCAP\TC107\TEST4.SYC. This trace was taken after making the changes to the NY router and bringing it back on line. The remote sites regained connectivity and did not experience any more disconnections.

Performance Tuning Exercise

Objective: Examine poor performance in a Novell NetWare WAN environment.

Background: The NetWare Supervisor is getting complaints from users that it takes a long time to log in to a remote Novell NetWare 3.11 file server. The file server and users are separated by a remote router link. The file server is a Simple Network Management Protocol (SNMP) Network Management Station (NMS) and is polling the user's local router. The ESIA is connected between the user's remote router and a packet network, synchronous modem.

1. **Load** the file C:\SYCAP\TC107\IPX_SNMP.SYC. Load the setups (**Files, Load, Setups**) file C:\SYCAP\TC107\IPX_SNMP.SYS. Display the data. As we saw earlier, in frame 35, the SUPERVISOR creates a connection with the NetWare server SXVGA and begins the login sequence.
2. In frames 43 and 45, do you notice any client/server negotiation inefficiencies which could affect performance?

Performance Tuning Exercise

Continued

3. Why do you suppose this is happening? (Hint: Look in the **Detail** window of frame 43. Notice the IPX header Transport control field Hop count. A hop count of 1 indicates this frame has crossed one router.)

4. Up to about frame 140 or so, does the session look normal?

5. Examine frames 905 to 949. Why do you suppose the login failed the first time in frame 912 and succeeded in frame 949?

6. How long does it take the user to successfully login?

Performance Tuning Exercise

Continued

7. If you were baselining how long it takes users to log on to the remote server, would you include the time you wrote down in question 6?

8. Turn off the NetWare protocol filter to display all protocols again. Go to frame 1. What else is happening over the WAN link?

9. How often does the polling cycle repeat?
   Does this seem excessive especially over a WAN link?

10. At this point we have gathered enough information to make some recommendations to improve performance over the wide area. What changes would you make to improve the login time?

Troubleshooting Exercise

Objective: Practice using the Sniffer Internetwork Analyzer to analyze and troubleshoot the cause of a slow response time problem.

Background: Users are complaining that when "Telnetting" to a host named TERRELL, it is taking forever to see what they type displayed on the screen. So far you have received trouble reports from the following IP addresses: 159.139.81.36, 159.139.81.32, and 159.139.81.41. The SIA is monitoring data over a bridged WAN link.

Hint: In this trace you will see Remote Who (RWHO) frames. UNIX servers running the (RWHO) daemon (background process) participate in periodically sending (RWHO) broadcast frames. The main purpose of RWHO frames is to update UNIX machines also running the rwho daemon as to which users are logged on to remote systems. Typing "**rwho**", part of the Remote Unix applications, at a UNIX console, returns a list of remote UNIX hosts, who is logged on to them, and the host's load average over time. UNIX hosts running BSD (Berkeley Software Distribution) version 4.2 send out an RWHO broadcast frame once a minute. In 4.3 BSD, the frame is sent once every 3 minutes.

Troubleshooting Exercise

Continued

1. **Load** the file: C:\SYCAP\TC107\SLOWRESP.SYC. Load the setups C:\SYCAP\TC107\SLOWRESP.SYS. (If you would like to see these setups look under **Display options**, **Protocol forcing**, **Rule 1**).
2. First we need to determine if the slow response time complaint may be the result of a congested WAN link. From the Expert Overview screen press **F2 View stats**. What is the average bandwidth utilization and the link speed?

3. Do you think purchasing or configuring additional bandwidth would significantly improve response time and eliminate the user complaints?

4. Press **F2 View expert**. Examine the two Applications layer diagnoses. For both Slow server diagnoses, press **Enter** until you reach the Application Detail screen. What other networking environment besides NFS is experiencing problems?

Troubleshooting Exercise

Continued

5. Which environment should you troubleshoot first? Which environment impacts more users?

6. We need to check the three Global Symptoms to see if some network-related problem is affecting performance. Press **Enter** to view the WANWide Symptom Summary screen. How often do the Broadcast/multicast storms occur?

   Write down the time each of the storms started.

7. Press **Enter** to view the WANWide Symptom Detail screen. Who and what protocol may be causing the Broadcast Storms?

8. Could the broadcast storms be related to the Retransmission and Slow server diagnoses? To find out, note the Start Time of each storm, turn on **Absolute time**, and **Search for text** on the Start Time of each of the storms. An alternative method would be to **Search for text** on "RWHO."

Troubleshooting Exercise

Continued

9. Could the retransmissions be caused by any physical or data link layer problems?
10. Now that we've ruled out a congested WAN link, and physical and data link layer problems as the cause of the slow response time complaint, let's investigate the Broadcast Storm diagnosis.
11. To isolate what type of broadcast/multicast traffic is responsible for the broadcast storm, set a display filter to show only broadcast frames. (Hint: **Display, Filters, Destination class**, turn off **Specific**.) What protocols do you mainly see?
12. What might explain why we see so many RWHO frames from host dev and host hdw?

    To find out, examine the source ETHER addresses. (Tab into the **Detail** window.) Which station sent the first RWHO frame in the first storm? Which station sent the rest?

Troubleshooting Exercise

Continued

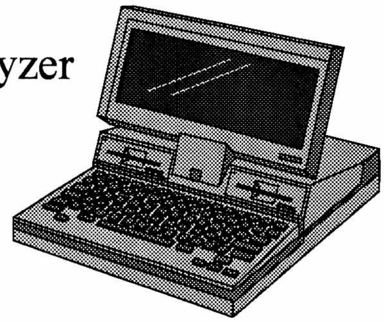
13. Examine the IP **Time to live** field in the **Detail** window of these packets as well. What is happening to the seconds/hop count?

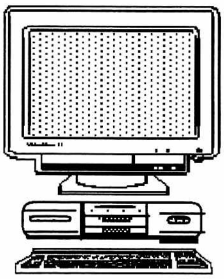
14. What steps would you take to resolve this problem?

NGC Product Information

LAN Analysis Tools

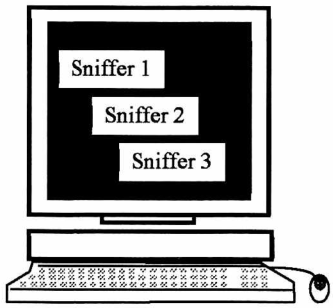
Expert Sniffer® Network Analyzer





Foundation Manager™

Distributed Sniffer System ®

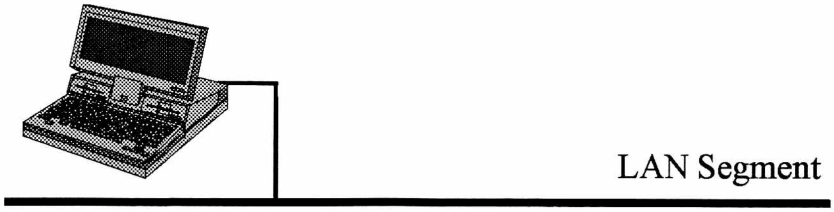


Expert Sniffer Network Analyzer

- Automatic identification of common network problems at all seven OSI layers in real-time
- Top-down view of the network, providing a end-user perspective
- Real-time configuration "learning"
- Explanations that recommend solutions to problems

Runs on Ethernet, Fast Ethernet, Token Ring, ATM, FDDI.

Sniffer Network Analyzer

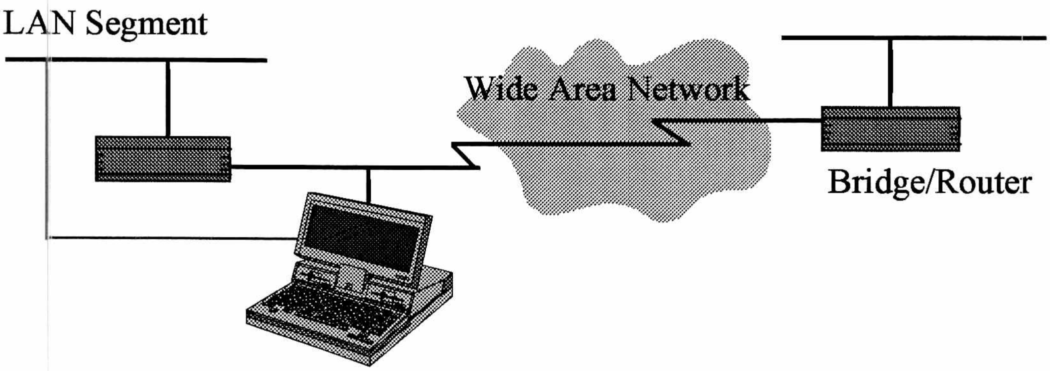


- Full 7-layer protocol analysis
- Complete suite of network protocols
- All popular network topologies
- Local and wide area network connections
- Advanced Monitoring: statistics, alarms and reports

Runs on Ethernet, Fast Ethernet, Token Ring, ATM , and FDDI.

LAN and WAN Connections

Extending the benefits of network analysis to the wide area



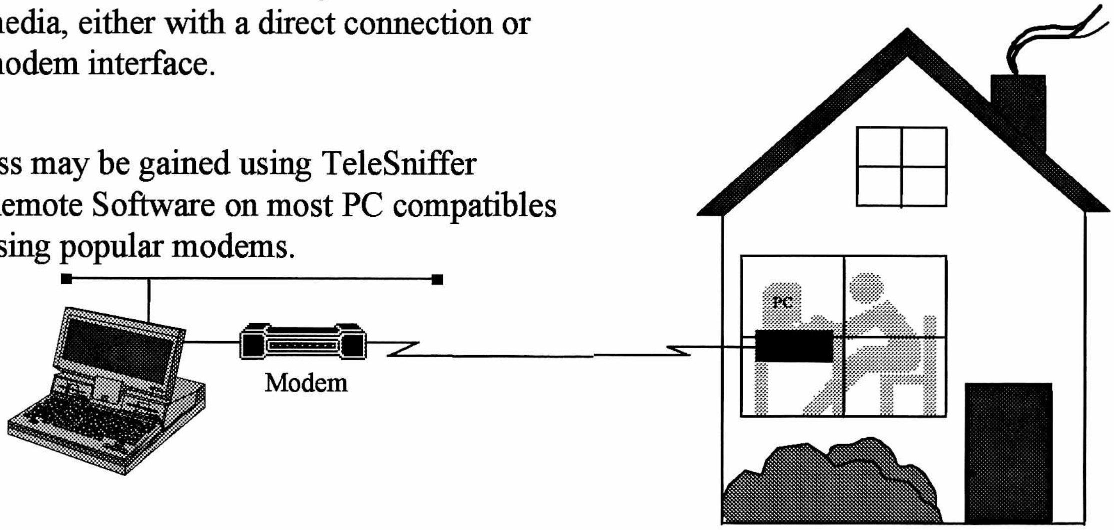
- Full 7-layer protocol analysis on your WAN:
  - Enables improved applications performance
  - Leads to decreased monthly line costs
  - Consistent user interface eliminates additional user training
  - Dual LAN/WAN support minimizes customer investment

Frame Relay, PRI/BRI ISDN, X.25, ATM, and more.

TeleSniffer

TeleSniffer software (DCA Remote2) is included with every Sniffer to allow remote access to the analyzer via RS-232 media, either with a direct connection or modem interface.

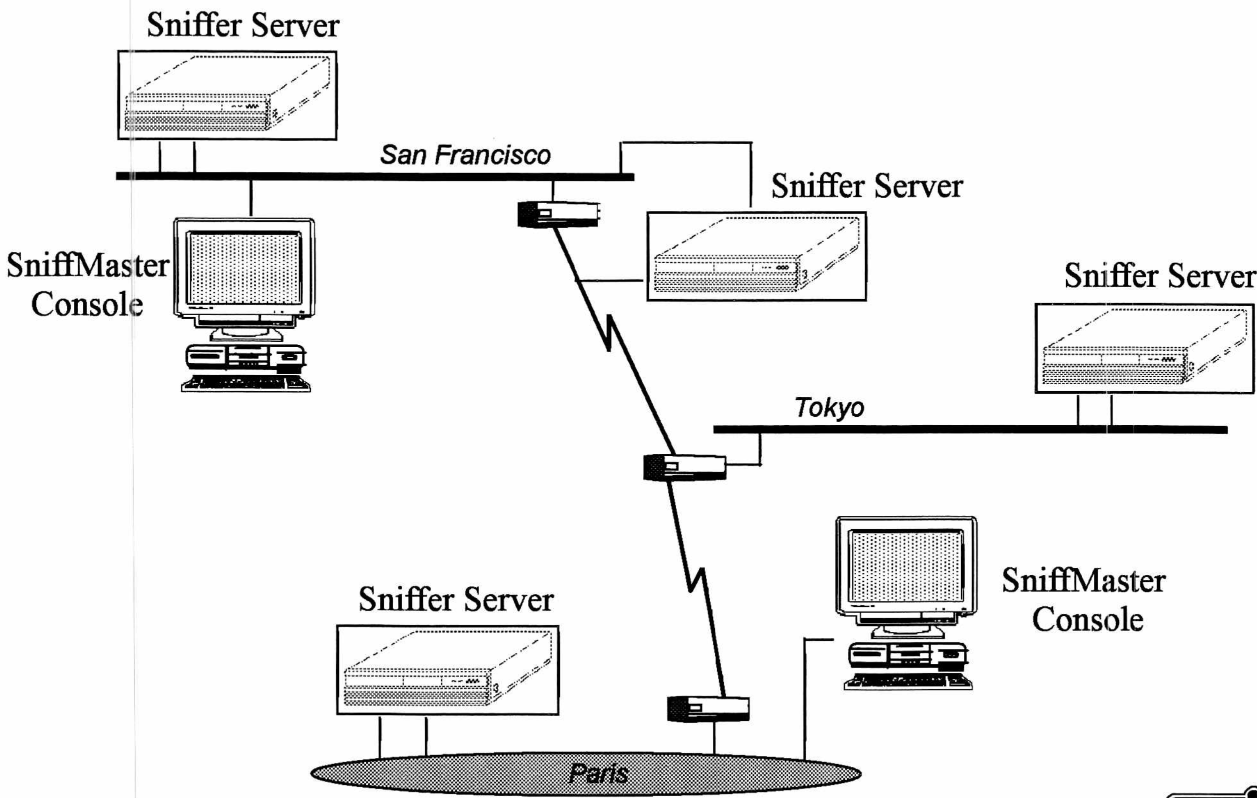
Access may be gained using TeleSniffer Remote Software on most PC compatibles using popular modems.



Can be used to troubleshoot a remote site. For example, Network General LAN Guru services uses it to troubleshoot customers' problems.

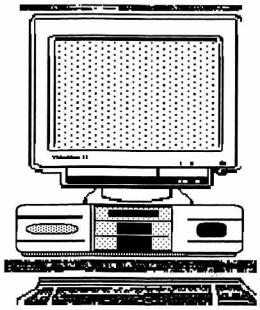
A very simple solution to remote analysis - not to be confused with the full-featured DSS solution which we will discuss in a few minutes.

Distributed Sniffer System



DSS allows remote operation of Sniffers over an internet, or out-of-band access.

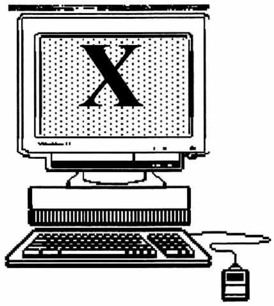
SniffMaster for WindowsConsole



- Provides simultaneous access to up to 30 Sniffer Servers.
- Consolidates alarm information from multiple Sniffer Servers.
- Downloads updates and new applications to Sniffer Servers.
- Provides centralized printer support.
- Both Ethernet and Token Ring Consoles are supported.
- The SniffMaster Console is available as a turn-key system or as a software-and-interface-board kit for use on any standard PC.

Supports up to 30 servers/Sniffers.

SniffMaster for X

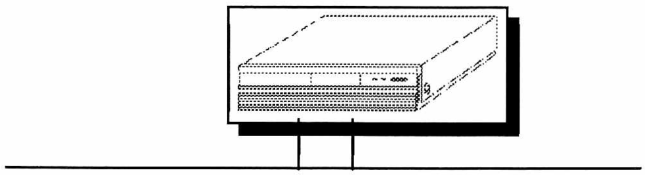


- Runs on a Sun SPARCstation with SunOS 4.1.x or later.
- Based on X-Window (X11.R4) and Motif Graphical User Interfaces (GUI).
- Simultaneous views of multiple Sniffer Servers.
- Mouse and Icon control of Sniffer Servers.
- Consolidated alarm log, using a separate window called the Alarm Viewer.
- Support for SNMP Traps.
- Communicates with Sniffer Servers using TCP/IP.

Supports up to 30 servers/Sniffers.

Distributed Sniffer Servers

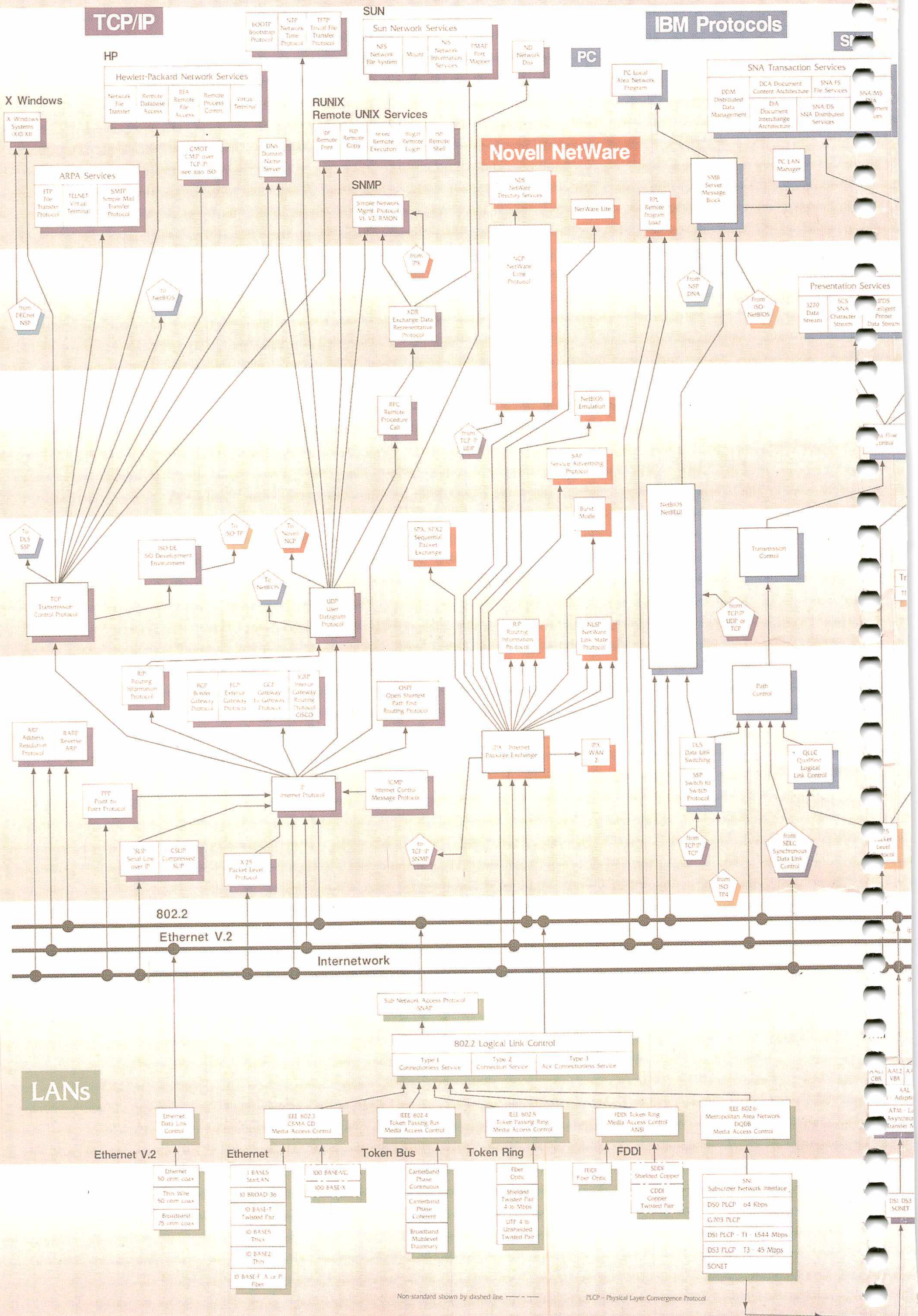
- Network interfaces for Ethernet, Token Ring and WAN.
- Analysis and Monitoring Applications for problem solving and performance optimization.
- Servers communicate with multiple SniffMaster Consoles.
- Statistics, alarms, and protocol information are stored on the Server to minimize network traffic.
- Servers communicate with consoles through bridged and routed networks



Server has the intelligence in the DSS - it captures and analyzes data. What it sends back to the console is actually just screen updates.

How to Contact Network General

- Technical Support - Have your serial number ready
  - (800) 395-3151
  - FAX: 415-327-9436
  - FAX-on-Demand: (800) 764-3329
  - Hearing Impaired Service: (415) 327-8723
  - Internet: support@ngc.com and http: //www.ngc.com
  - FTP through the Internet to host NGCGATE.NGC.COM
  - CompuServe: type GO NETGENERAL at any ! prompt
  - SniffNet Bulletin Board (415) 327-3875 < 14.4 K bps
- Sniffer University
  - (800) 395-3151
  - FAX: (415) 327-8780
  - FAX-on-Demand (800) 764-3329
  - Internet: snifferu@ngc.com and http:// www.ngc.com


TCP/IP
SUN
Sun Network Services
IBM Protocols
HP
Hewlett-Packard Network Services
X Windows
RUNIX
Remote UNIX Services
PC
Novell NetWare
SNA Transaction Services
ARPA Services
SNMP
Presentation Services
802.2
Ethernet V.2
Internetwork
802.2 Logical Link Control
LANs
Ethernet V.2
Ethernet
Token Bus
Token Ring
FDDI
Non-standard shown by dashed line
PLCP - Physical Layer Convergence Protocol